TABLE OF CONTENTS

Colonel Edwin C. Roessler Jr.

Fairfax County Police Department

Colonel Edwin C. Roessler, Jr. serves as Chief of Police of the Fairfax County Police Department, following his appointment on July 30, 2013, and has 31 years of law enforcement experience. Colonel Roessler previously served as Deputy Chief of Patrol managing crime fighting efforts across all eight district stations in a county of 400 square miles serving over 1.2 million community members. One of Colonel Roessler's first actions as Police Chief was to form the Chief's Council on Diversity Recruitment. The Council engages community leaders to guide and advise the Chief and the Department's leadership team on how to achieve recruitment goals and better represent Fairfax County's culturally diverse communities within the sworn, civilian, and volunteer workforce; while also creating and nurturing a robust dialogue with all communities served. The strategic plan for diversity recruitment embraces the Department's ongoing goal of improving engagement with the community to prevent and fight crime, improve the culture of safety both internally and in the community, and to keep pace with urbanization.

Colonel Roessler's prior senior command assignments included the Internal Affairs Bureau, the Criminal Justice Academy, the Administrative Support Bureau, and a Patrol Bureau division. Colonel Roessler currently serves as a senior advisor to the International Association of Chiefs of Police for its International Police Education and Training program in partnership with the United States Department of State and the American University. Colonel Roessler serves as the chairman of the Federal Bureau of Investigation's taskforce for the conversion to NIBRS as well as serving as the representative to the Bureau's CJIS Advisory Panel Board as the representative of the Major Cities Chiefs.

Recently Colonel Roessler has increased public safety employee wellness endeavors locally and nationally through innovative suicide prevention and awareness programs led by the Major Cities Chiefs Association, the Department of Justice, and several not for profit organizations. Colonel Roessler also continues to build upon transparency with his community and co-producing transformational organizational change with all community and department stakeholders in critical areas such as use of force, responding to mental health calls for service, and meeting the needs for the delivery of essential police services that rapid urbanization produces.
Colonel Roessler received his undergraduate degree from Arizona State University and his graduate degree from the George Washington University. Colonel Roessler has graduated from a variety of professional development programs including: the Federal Bureau of Investigation's National Executive Institute and National Academy, the American University's Key Executive Graduate Program, the United States Military Academy West Point Leadership Program, and

Leadership Fairfax. Colonel Roessler's professional affiliations include the International Association of Chiefs of Police, the Major Cities Chiefs, the Virginia Association of Chiefs of Police, the Major Cities Chiefs Human Resources Committee, the Police Executive Research Forum, FBI National Academy Associates, and the Society for Human Resource Management.

Colonel Edwin C. Roessler Jr.
Fairfax County, Virginia Police Department

Strategic Recommendations for Building Public Trust and Successes with Body Worn Cameras

April 21, 2020

During the summer of 2014 several controversial officer-involved shooting (OIS) events and other less-lethal use of force incidents were captured on both community member and law enforcement video platforms which includes cell phones, police cruiser in-car videos, and officer body worn cameras (BWC). The video footage from these police-community member interactions went virial on both social and mainstream media networks eroding the public's trust of law enforcement nationwide. These events were a watershed moment in American law enforcement as many local governing bodies directed their law enforcement leaders to purchase BWC's immediately following the incidents with the collective goal of increasing police accountability in their communities. Law enforcement and political leaders must understand that attaining increased accountability using BWC's must be planned strategically before the phases of final procurement, implementation, and refresh of the evolving technologies occurs to sustain long-term goal successes.

As many law enforcement leaders reacted to the cumulative loss in the public's trust due to widely publicized use of force events, they used creative procurement processes, including grant opportunities, to quickly buy "off the shelf" BWC equipment to rapidly deploy them in the field. These reactionary procurements and deployments lacked basic strategic planning principles such as; academic study, training, testing and evaluation, analysis of data storage, compatibility with existing records management systems and information technology environments, Freedom of Information Act (FOIA) compliance, long term budgeting concepts to sustain the new line of business, and many ignored the opportunities to co-produce these strategies with community advocates and criminal justice system stakeholders. In just two years a majority of law enforcement agencies that were quick to stand up their BWC programs became failures and further eroded the public's trust of the law enforcement profession as they were unable to sustain BWC programs across core business modes due to a lack of strategic planning. These agencies quickly realized the BWC system had tangible and intangible costs both administratively and operationally and these factors continue to be obstacles for successes needed to properly leverage BWC technology in a majority of the 18,000 law enforcement agencies in the United States of America.

Understanding the critical need to strategically plan for the implementation of a BWC system across all strategic objectives outlined above, in the summer of 2014 the Fairfax County Police Department was determined to study BWC best practices and analyze challenges and failures experienced by other departments to design a pathway to success for their BWC program. The following is a briefing of the core foundational components recommended to strategically build a successful and sustainable BWC program that will build upon the public's trust by increasing accountability through transparency in an effort to reduce use of force incidents while holding the public accountable for their interactions with law enforcement.

Co-Production of Policing for BWC Policy

The co-production of policing is a concept in which all stakeholders meet to develop policy recommendations for the administrative and operational goals of the law enforcement agency. In regards to the development of a BWC program policy, its recommended that both formal and informal groups be able to make recommendations to the chief of police on such factors as when to turn the BWC on and off, what other officers besides patrol officers should wear BWC's, when should footage be released or withheld, and how long certain footage should be retained beyond legal retention requirements. In Fairfax County the advocacy group met with a police commander while other parts of the BWC program were strategically being built. The group made a consensus recommendation of a final policy which was then put to the test in a pilot program and then studied for effectiveness by an academic institution. The advocacy group for the policy was then adopted as a permanent group to review the BWC policy on an annual basis to ensure the program meets the transparency and accountability needs of the communities served.

The co-production model used to develop the policy also ensured the maximum levels of transparency by agreeing to a pre-disposition to disclose when the footage release would not impact the integrity of the criminal and/or administrative investigations and that FOIA would only be used to protect the integrity of the investigation and/or human decency factors.

Stakeholder Leadership Advisory Group

All BWC programs need an IT infrastructure and program assessment by local criminal justice system staff (i.e. prosecutors, public defenders, judges, and clerks). Therefore, its critical to socialize the BWC endeavor through the creation of a user group made of local criminal justice system leaders as there are in-direct costs to a police department to buildout the IT infrastructure to work beyond the police operational environment. The other criminal justice agencies also need to strategically plan and budget for adopting the BWC program in their environments.

Competitive Procurement Process for Testing and Evaluation

Based upon national and international BWC program failures, it was determined that the Fairfax County Police Department would use the competitive procurement process to find suitable vendors to test and evaluate BWC systems at three different unique policing environments as determined by geographic locations, use of force data, demographic data, and rapid urbanization environments (i.e. rail, retail, high rise, night life etc.). This allowed for operational and administrative analysis to determine the actual scope of the specifications of the product that would best fit our IT infrastructure.

Academic Study

In order to measure all metrics without bias, the Fairfax County Police Department allowed itself to be studied before, during, and after the pilot project to make informed decisions to enter the BWC program procurement process. The study was achieved ensuring the highest level of academic rigor and transparency. This was evidenced as the study was truly independent as no monies were exchanged for research services and the Chief of Police and other leaders were not privy to the researchers as they conducted their studies.

Although the study demonstrated that BWC's in Fairfax County did not alter the public's trust, it significantly determined that BWC's made a difference with both the community and police officers in holding each other accountable for interactions.

Project Implementation Plan

Using the co-production of policing model across all strategic objectives, the final pilot project study report by the academic institution was delivered in an official public meeting with elected officials and all stakeholders in order for the most informed decision(s) to be made to authorize funding to move ahead with the procurement and implementation processes.

The pilot project and academic study was critical in designing the scope of the needs for the local government IT infrastructure, user needs, and stakeholder needs. This is the foundation of sustainability. The stakeholder teams remain as an official process with the academic institution to continue to monitor the BWC program across all lines of business and policy in order to make refinements and prepare for the renewal of a contract prior to the expiration of the current 5-year vendor contract.

The criticality of continuous measurement of the BWC program across many metrics is now supporting the scope and design of re-engineering other IT platforms to strategically plan an integration project to build one IT system that will coordinate all the data from in-car videos, BWC's, records management, workload data, and other emerging technologies. The metrics will continue to help us met our vision statement of preventing and fighting crime, preserving the sanctity of all life, and keeping pace with rapid urbanization.

Public Accountability Strategic Uses for BWC Programs

Nationally there is a struggle to understand from an academic standpoint as to whether or not BWC programs actually make a difference in law enforcement behaviors regarding discourteous behavior, reduction in police use of force incidents, and improved procedural and equitable justice administration to avoid dis-portionality in policing.

The academic review of the Fairfax County Police Department's BWC pilot project community and user surveys did not indicate any statistically significant data to suggest that BWC's made a difference. However, as mentioned above, it's the fact we had the BWC's that made both community members and officers feel more confident in policing accountability to build upon our great public trust.

Consideration must be given to leveraging the accountability of all technologies to build public trust department-by-department to improve the national public trust of law enforcement. The example of Fairfax County's co-production of policing model to build a BWC program is a highly recommended first step to providing a sense of ownership to the community to ensure essential police services meet all stakeholder needs. The next step of using video technology to improve the public's trust after deployment of BWC programs specifically, is integrating all technologies with transparency methodologies whereby there is an actual standardized process to review without bias, the video footage from all IT sources. The viewing of all video footage procured from IT sources must also comply with applicable laws and the Police Officer's Bill of Rights in each jurisdiction. Some crucial examples of the careful consideration needed in all reviews of video footage include questions such as: when officers should view their videos after critical events such as an OIS, when to (and what to) release to the community following critical events, policies for allowing civilian review panel to access video footage for their reviews of complaints, and access to video footage by police auditor systems.

Thank you for the opportunity to brief all of you on the strategic recommendations of how to use the co-production of policing model to successfully build and sustain a BWC program with community stakeholders to enhance public trust in the law enforcement profession.

FAIRFAX COUNTY POLICE DEPARTMENT'S BODY-WORN CAMERA PILOT PROJECT: AN EVALUATION

Richard R. Bennett, Ph.D. Brad Bartholomew, Ph.D. and
Holly Champagne, J.D.

Department of Justice, Law and Criminology
The American University
Washington, DC

This research was made possible through generous grants from the School of Public Affairs at American University and the Charles Koch Foundation. The views expressed in this document are those of the authors and do not represent either funder.

The authors thank Sandra Baxter, Ph.D., Bill Harder, Ph.D. and Eric Schuler, Ph.D., of American University for their contributions to the study and this final report.

The authors also thank FCPD Majors Christian Quinn and Chantel Cochrane for their outstanding support and for facilitating our access to many units within the department. We also acknowledge the assistance of the commanders at the three police districts in which the pilot project was undertaken. We are especially grateful to the analysts who compiled information on officer activities and police-community encounters. Finally, we thank the police officers and community members who so graciously participated in this study.

Questions about the evaluation should be directed to Prof. Richard Bennett (bennett@american.edu) or Prof. Brad Bartholomew (bartholo@american.edu).

CONTENTS

Final Report: Fairfax County Police Department's Body-worn Camera Pilot Evaluation Study

June 2019

EXECUTIVE SUMMARY

In 2017, the Fairfax County (Virginia) Police Department, known as FCPD, decided to launch a pilot implementation of body-worn cameras (BWCs) to learn what the technology involved, the response of its officers to it, what community members and local organization leaders would think, and the changes in policing practices and outcomes that would occur. Some police agencies in the Metropolitan Washington, DC area had already adopted BWCs and there was a push nation-wide to implement them quickly in the face of numerous high-profile and controversial interactions between police and citizens. FCPD officials wanted to proceed more cautiously and conduct a BWC pilot program first. They asked a team of researchers at American University in Washington, DC, to assist them.

The formal evaluation began before and continued after the six-month pilot period when Squad B officers in three districts were assigned BWCs and Squad A officers in those same districts continued their duties without them. The study design included 17 data collection efforts: paper surveys of police officers at those districts before and after the pilot, an on-line survey of community stakeholders, a telephone survey of 609 community members who had interacted with officers during the pilot, 12 focus groups with officers and supervisors during and after the pilot and approximately 70 hours of ride-a-longs with FCPD officers. The results from analyses of all those data are presented below.

PERSPECTIVES OF THE POLICE OFFICERS:

The officers' attitudes regarding BWCs were very consistent across the two squads and across the two surveys with no significant differences found. There was consensus that BWCs will increase the gathering of evidence, help settle complaints against officers and increase the department's transparency to the public. Their responses were more mixed on whether BWCs will make officers more professional or reduce proactive encounters with the public. They disagreed that BWCs will improve their legitimacy among community members, improve community relations generally or increase officer safety.

A key question asked about adoption of BWCs throughout the department. Both Squad A and Squad B officers held similar opinions at Time 1, but at Time 2, their opinions differed significantly: Squad B officers were slightly more in favor of adoption while, Squad A officers were dramatically less favorable towards adoption.

Comments gathered from the 12 focus groups provided insights helpful in interpreting the survey results. A notable number of participants contended that BWCs are needed only by departments with serious community relations problems, violent incidents or corruption. Believing that none of those descriptors fit FCPD, they wondered why BWCs might be implemented in Fairfax County. There was a belief among some officers that BWCs and pay raises would be paid from out of the same "pot" in a zero-sum manner. Given the choice, they preferred ("long overdue") raises. Most officers believed their behavior and that

of community members did not change because of BWCs. They acknowledged initial resistance to BWCs, but said it has decreased with familiarity over time. They believed that BWC recordings have positively and negatively affected justice system operations. They appreciated the improvements BWCs bring compared with in-car videos, recognized the additional work required by staff and the reality that BWCs are not perfect.

DATA ON OFFICER PERFORMANCE:

Officer performance data were gathered from the department's own records concerning the number of traffic stops, other incidents, citizen complaints and use of force reports documented before, during and after the pilot period. Statistical analyses revealed no indications of de-policing during or after the pilot period. Both Squad A and Squad B officers continued their normal performance profiles with regard to traffic stops and responses to both violent and non-violent incidents. Similarly, there was no change in use of force in general, direct force, indirect force or use of force by pointing a firearm.

Significant statistical changes were found, however, in citizen complaints during the post-pilot period. On average over each two-week period, complaints declined by 0.4 complaints for Side B officers with BWCs and increased by 0.2 complaints for Side A officers. While statistically significant, these effects should not be over interpreted because the number of overall complaints is small.

PERSPECTIVES OF COMMUNITY STAKEHOLDERS:

The community stakeholders provided a valuable perspective on the BWC pilot program in addition to their assistance on BWC policies. Less than half of them agreed that BWCs would reduce complaints against police officers, make the police more legitimate in the eyes of their community members or lessen the use of force. Only the statement that BWCs would make the police more accountable was agreed to by more than half of the stakeholders. Clearly, the use of BWCs alone was not seen by the stakeholders as a way to resolve community-police problems.

The distinction between stakeholders heading up government-related organizations and those leading non-governmental organizations (NGOs) proved useful. The NGO leaders were much more positive about the effects of BWCs than were the government-based leaders. The NGOs unanimously agreed that BWCs will reduce complaints against police officers and make the police more accountable. The majority of them also agreed that BWCs would make the police more legitimate in the eyes of their community members and would lessen police use of force. None of these four statements were agreed to by more than two-fifths of the government stakeholders. When presented with three statements about the FCPD, however, the vast majority of both groups were positive. Nearly three-fourths of the government sub-group agreed that they were adequately involved in making BWC policy for the pilot, that FCPD shares the values of their community and does its job well. More than four-fifths of the NGOs did too. It would be interesting to learn why the government stakeholder are underwhelmed by the likely positive effects of BWCs and why the NGOs are so optimistic.

PERSPECTIVES OF COMMUNITY MEMBERS:

A total of 603 community members participated in a telephone interview regarding their recent interactions with an officer, either wearing a BWC or not, during the pilot period. The majority of respondents expressed satisfaction regarding the interaction. For example, strong majorities reported being satisfied with how the officer treated them and with how the encounter with the police was resolved. Nearly all of those surveyed believe that the officer treated them in a procedurally just manner

by acting respectfully, fairly, professionally and by listening to the respondent's side of the story and talking about the decisions being made. These findings indicate that on a personal level, the majority of those who interacted with an FCPD officer during the pilot period recalled the interaction in a positive light.

The majority of respondents also viewed FCPD in a positive light. Strong majorities believe that FCPD does its job well and that FCPD shares the values of the respondent's community. In other words, among community members who had a recent interaction with the police, most of them report feeling positive not only about their personal experience but also about the department as a whole.

Further, there is overwhelming support among these community members for the widespread adoption of BWCs. Interestingly, there is no evidence that the presence or absence of a BWC during their police encounter had a meaningful impact on their satisfaction with the interaction or the FCPD.

Finally, both the age and race/ethnicity of the community member appear to influence their perceptions. Although majorities of all age and racial/ethnic groups report mostly positive feelings regarding both their personal interactions with an officer and toward FCPD, there are noticeable differences. Older community members are more likely to recall their interaction and the FCPD in a positive light than do their younger counterparts. The same was true for race/ethnicity, with Caucasian and Asian community members expressing more positive feelings about their interactions and FCPD than do African Americans, Hispanic and Native Americans. Surprisingly, this finding was somewhat reversed when the question turned to whether BWCs should be worn by all officers. The largest percentages of "strongly agree" responses is among young adults (ages 18 to 24) and three race/ethnic minority groups (African Americans, Asians, and Native Americans) but when the percentages that strongly agreed and agreed are combined, no group stood apart from the others.

Section One: Introduction

Section One: Introduction

In 2017, the Fairfax County (Virginia) Police Department, known as FCPD, decided to launch a pilot implementation of body-worn cameras (BWCs) to learn what the technology involved, the response of its officers to it, what community members and local organization leaders would think, and the changes in policing practices and outcomes that would occur. Many police agencies in the local Washington, DC area had already adopted BWCs, and there was a push nation-wide to implement them quickly in the face of numerous high-profile and controversial interactions between police and citizens. FCPD officials wanted to proceed more cautiously and conduct a BWC pilot program first.

PART A. THE SCOPE OF FCPD'S PILOT PROGRAM AND ITS EVALUATION

The evaluation efforts underlying this report began in August 2017 when the FCPD invited an American University research team to advise them on the study design for a six-month pilot test which would be rigorous, comprehensive, informative and actionable. The resulting study design was a quasi-experimental randomized trial based in three of the department's eight districts. The evaluation timeline called for multiple data collection efforts before, during and after the pilot test and sufficient time afterwards to analyze the data and prepare this report.

Only a few documented BWC evaluation projects have used a true random controlled trial design because that caliber of the design requires that individual officers be chosen to wear BWCs through a random selection process. Like most police agencies, FCPD has long assigned their officers to squads, and dismantling squads for the sake of the pilot program was not feasible. Instead, the research team and department officials decided to take advantage of the two-squad structure already in place, Squad A and Squad B. An official flipped a coin, a classic way to do random selection, and it landed on "tails." Thus, Squad B became the treatment group for the pilot project and its members were assigned BWCs and trained how to use them. Squad A became the control group and received neither. The final study design choice to be made concerned how many and in which districts to base the program. The decision was collectively made that three specific districts serving very different communities would provide a sufficiently realistic test.

The research team and FCPD officials then began identifying the key design components. The FCPD had successfully collaborated with community stakeholders in the past to get birds-eye feedback on local needs and concerns. A group of stakeholders was identified for the pilot program and FCPD worked closely with them in formulating BWC policies which would address personal privacy rights and constitutional safeguards for community members and police officers alike. It was decided that the researchers would survey them early in the pilot program.

Three additional data collection activities were undertaken. Qualitative and quantitative data were to be collected from officers in both squads via focus groups and surveys before, during and after the pilot. Another set of data was collected from community members that engaged with Squad A and Squad B officers in the field during the pilot period. Finally, field data were collected on officer activity in the three pilot districts along with complaints against officers and officer use of force reports. This required a challenging coordinated effort between the department's official records staff and a team of telephone interviewers working in four languages from the university's campus.

PART B. EVALUATION APPROACH AND METHODOLOGY

Figure 1.1 Design of the Evaluation Study

The set of concentric circles in Figure 1.1 illustrates both how the researchers designed the evaluation and how this report is organized. The researchers conceived of the FCPD as having four important audiences, internal and external, whose attitudes and experiences constitute the full context of the pilot program. The inner circle connotes the use of BWCs by the department during the pilot period.

The second ring is comprised of the police officers themselves, some of whom (Squad B officers) were selected to wear the cameras during the six-month pilot. Their attitudes toward and experiences with using BWCs in the field, when contrasted with those of Squad A officers, their non-BWC wearing colleagues, was viewed as the most informative feedback in the study. The research design thus included multiple data collection efforts focused on them using both qualitative (i.e., focus groups and ride-a-longs by a researcher) and quantitative (i.e., paper and pencil surveys) research methods.

The third ring is comprised of officer performance data gathered from the department's records concerning the number of traffic stops, other incidents, citizen complaints and use of force reports documented before, during and after the pilot period. The formal records also indicate the squad identification of every officer involved in the events. These data define the performance context of the pilot.

The fourth ring includes community members who engaged with officers during the pilot period. Their feedback on satisfaction with how they were treated, how the situation was resolved, and how they regard the FCPD, among other issues, also constitutes a key context for the evaluation. The researchers conducted telephone interviews with community members as soon after their interactions with police officers as possible. The squad identification of the officers involved was also noted by the researchers.

The fifth and outer ring includes community stakeholders, such as heads of government-related organizations, business groups, faith communities and neighborhood organizations, whose expansive knowledge of their community members' policing concerns, experiences and attitudes was deemed important and worth collecting via a survey before the pilot period began.

PART C. SPONSORSHIP OF THE EVALUATION

The School of Public Affairs and other offices within American University provided significant support of many types. The School of Public Affairs funded the community member telephone survey portion of the project. Members of the university's Institutional Review Board examined all consent forms and data collection instruments to make sure they were justified, appropriate and protected the welfare and rights of the intended survey respondents and focus group participants. Officials within the Office of Campus Life & Inclusive Excellence were invaluable in our recruitment of student interviewers who were fluent in English as well as Spanish, Korean and Vietnamese. University staff made space and equipment available for the interview team to do its work

The Charles E. Koch Foundation provided additional financial support for the research team's work in completing the evaluation. The Foundation has long supported studies on body-worn cameras and other police reform efforts.

PART D. OVERVIEW OF THE REPORT

In addition to this Section One, the report includes five subsequent sections:

- Section Two: Perspectives of the Police Officers presents the results from the surveys and focus groups conducted with Squad A and Squad B officers as well as insights from ride-a-longs.
- Section Three: Organizational Data on Officer Performance details the official FCPD records used to ascertain whether four measures of performance (the number of traffic stops made, incidents investigated, community complaints received and uses of force reported) changed over the pilot period or afterwards for Squad A and Squad B officers.
- Section Four: Perspectives of Community Members reports the results from a telephone survey of community members that engaged the police officers during the pilot period.
- Section Five: Perspectives of Community Stakeholders present the results from a pre-pilot survey of stakeholders on their attitudes toward BWCs and the FCPD.
- Section Six: Synthesis of Evaluation Results and Study Conclusions provides an integration of all research conclusions presented in the four prior sections and conclusions about the BWC pilot program.
- There are seven appendices.

Section Two:
Perspectives of the Police Officers

Section Two:
Perspectives of the Police Officers

SUMMARY OF FINDINGS:

- The group of officers that participated in the pre-pilot survey were similarly split among Squad A (41%) and Squad B (41%), with the remainder assigned to neighborhood patrol units, animal control or motorcycle units.
- Analyses tested whether the demographic profile of Squad A officers differed from that of Squad B officers to a statistically significant degree. There were no differences in their years of experience, gender, race/ethnicity or education; characteristics which might predict attitudes towards BWCs.
- There was no difference in attitudes between Squads A and B in their acceptance of BWCs just before the pilot program began. By its end, the two squads held significantly different attitudes: Squad A was more negative while Squad B was slightly more positive compared to their initial attitudes.
- Overall, the officers' attitudes varied based on the type of impact they anticipated BWCs making. A majority of Squad A and Squad B officers agreed that:
    - BWCs will help to gather evidence (A: 80%, B: 91%).
    - BWCs will help settle complaints against them (A: 80%, B: 86%).
    - BWCs will increase the transparency of the department (A: 44%, B: 50%).
- A majority of Squad A and Squad B officers disagreed that:
    - BWCs will improve their legitimacy (A: 53%, B: 69%).
    - BWCs will improve relations between police and the public (A: 44%, B: 53%).
    - BWCs will increase officer's safety (A: 52%, B: 54%).
- A majority in both squads were unsure whether:
    - BWCs will make police officers more professional.
    - Officers will reduce proactive encounters with community members.
- Many focus group members wondered why BWCs are needed in a police department with such high levels of professionalism and low levels of problems as FCPD.
- There was initial resistance to BWCs, which may have partially stemmed from a misperception that BWCs and pay raises are paid from the same budget category.
- Officers believed that both their behavior and that of community members would not change due to BWCs.

PART A. SURVEY METHODOLOGY

The officers from the three treatment districts were surveyed prior to their knowing which squad would be issued the BWCs (Time 1) and just after the cameras were no longer deployed (Time 2)[1]. The paper and pencil surveys were administered in person at the officer's roll call or debriefing sessions. The surveys were administered at nearly the same time in the three districts. A total of 29 questions were asked in five content areas: Community Members Behavior, Police Officer Behavior, Evidence Usage, General Perceptions of Camera Usage and Recommendations concerning adopting the BWCs. The response rate varied by district.[2] Several selected questions asked in the first four areas will be explored by comparing officers who received the cameras (Squad B) and those who did not (Squad A) both before being assigned a BWC (Time 1) and after the pilot terminated (Time 2). Figures 1 through 5 present the officer demographics.

PART B. ANALYSES OF THE SURVEY DATA

Figure 2.1 shows officer assignment. Forty-one percent of the respondents to the survey indicated that they are assigned to Squad A and 41% of the respondents are assigned to Squad B. The remaining 18% of respondents are assigned to specialized units like the Neighborhood Patrol Units (NPU), Animal Control and Motorcycles.

Figure 2.1: Officers' Current Assignment

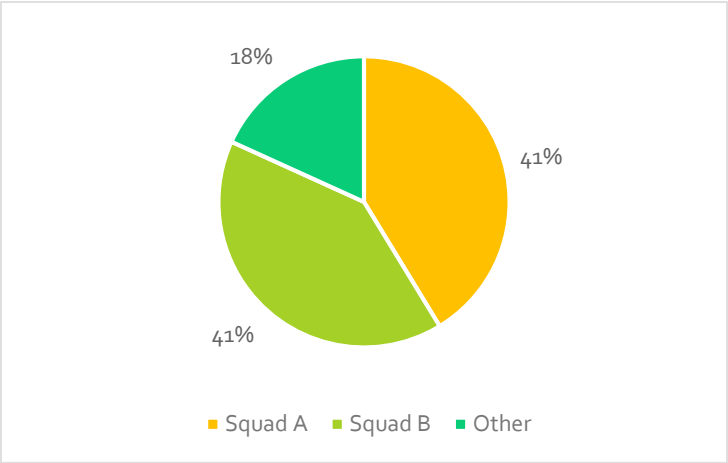


Figure 2.2 presents the years of experience the respondents have as police officers. Twenty-eight percent of the respondents are new to the occupation with years of service ranging from less than one year to 4

[1] The officers in the three districts were first surveyed (Time 1) on January 30th and 31st, 2018. The second administration (Time 2) took place October 2nd and 3rd. The two-day sequence was used so that both squads could be surveyed as close together in time as possible.

[2] The response rate for Mason at Time1 was 94% and Time 2 was 85%: for Mt. Vernon at Time 1 was 87% and at Time 2 was 73%; for Reston at Time 1 was 88% and at Time 2 was 83%. The reductions in response rate between Time 1 and Time 2 are particularly due to the replacement of personnel in the Districts. When new personnel were assigned to the district who had not participated in the first round of surveys, they were asked not to complete the Time 2 survey.

years. The largest group of officers (32%) have served Fairfax County for more than 17 years. The other three age categories contain similarly small percentages of respondents. A Student's t test was performed to determine if Squad A and B differed on their age composition. Figure 2.3 shows that there is no significant difference in age composition by respondents.

Figure 2.2: Officers' Years of Experience

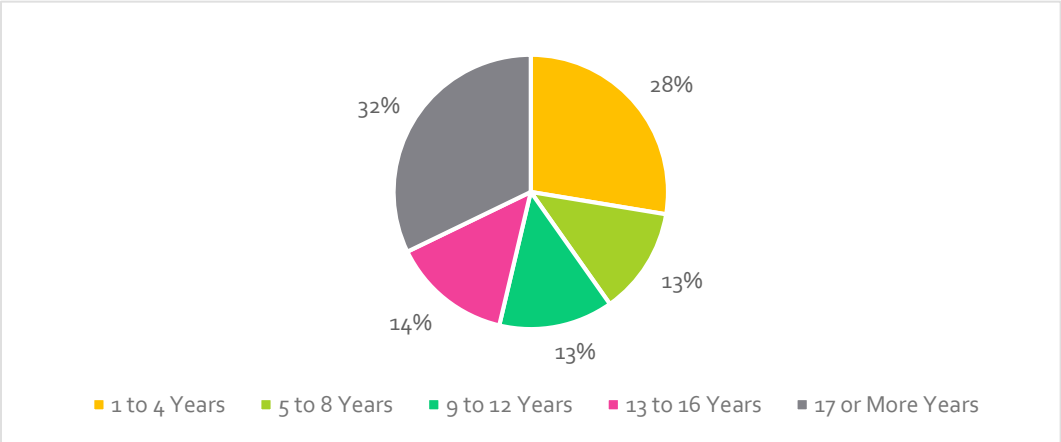


Figure 2.3: Student's t Test Showing the Comparison between Squads A and B at Time 1 to Determine if They Differed on Years of Experience

	N	Mean	SD	SEM	t	Results
Squad A	100	11.3525	8.34901	0.83490	-1.162	Not Sig.
Squad B	157	12.5669	7.87118	0.62819		

Figure 2.4 presents the gender composition of the respondents to the survey. The vast majority of respondents are men (86%) while women make up only 12% of the respondents. Finally, 2% identify themselves as neither a man nor woman. Again, a Student's t test was performed to see if the gender composition of Squads A and B differed. The findings in Figure 2.5 indicate that the gender composition is not significantly different.

Figure 2.4: Officers' Gender

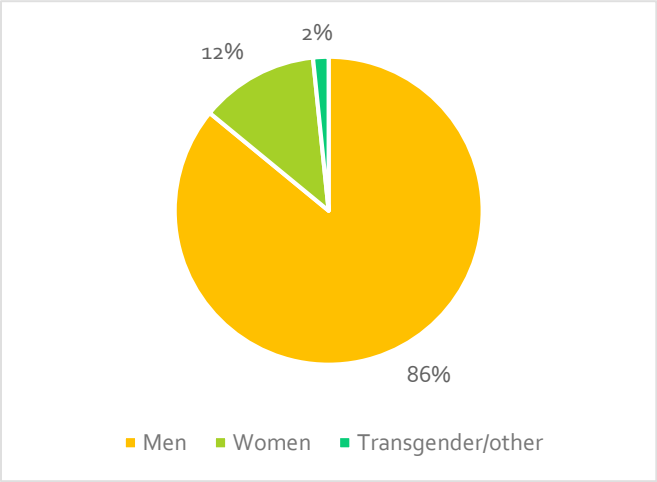


Figure 2.5: Student's t Test Showing the Comparison between Squads A and B at Time 1 to Determine if They Differed on Gender

Squad	N	Mean	SD	SEM	t	Results
A	99	1.16	0.422	0.042	-0.585	Not Sig.
B	160	1.19	0.442	0.035		

Figure 2.6 shows that the racial/ethnic composition of the respondents is dominated by Caucasians (77%) followed by Hispanics (7%). African Americans and Native Americans each accounted for 6% of the respondents, Asians account for 4% of the respondents and less than 1% of the respondents identify themselves as other. Again, a statistical test was used to determine if the racial/ethnic composition of Squad A differed from respondents in Squad B (see Figure 2.7). The test yields a t value of 1.167 which does not reach the .05 level of probability commonly used in social science research.

Figure 2.6: Race/Ethnicity of Police Officers

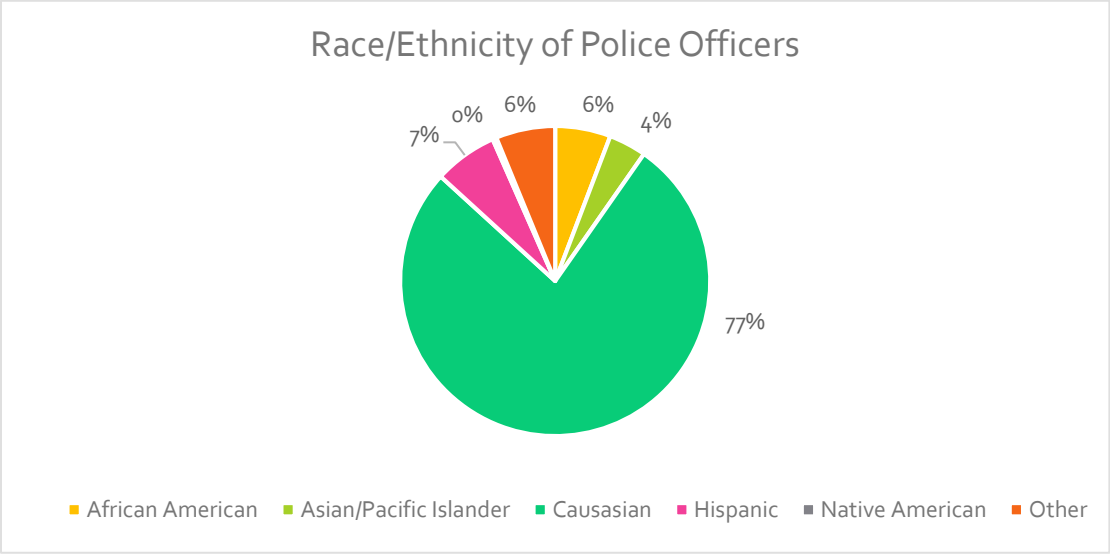


Figure 2.7: Student's t Test Showing the Comparison between Squads A and B at Time 1 to Determine if They Differed on Race/Ethnicity

Squad	N	Mean	SD	SEM	t	Results
A	97	3.12	0.832	0.085	1.167	Not Sig.
B	156	3.08	0.964	0.077		

The final officers' demographic characteristic explored is their educational level. Figure 2.8 presents the findings on officers' educational accomplishment. The majority of FCPD officers (55%) have a four-year college degree and impressively, 8% of the officers have an advanced degree. Twenty-two percent of the respondents have some college while 10% have a two-year degree. Only 5% of the pilot program officers have a high school or GED diploma. A statistical test was run to determine if the educational level of Squad A differed from respondents in Squad B. Figure 2.9 shows that there is no statistical difference.

Figure 2.8: Officers' Educational Level

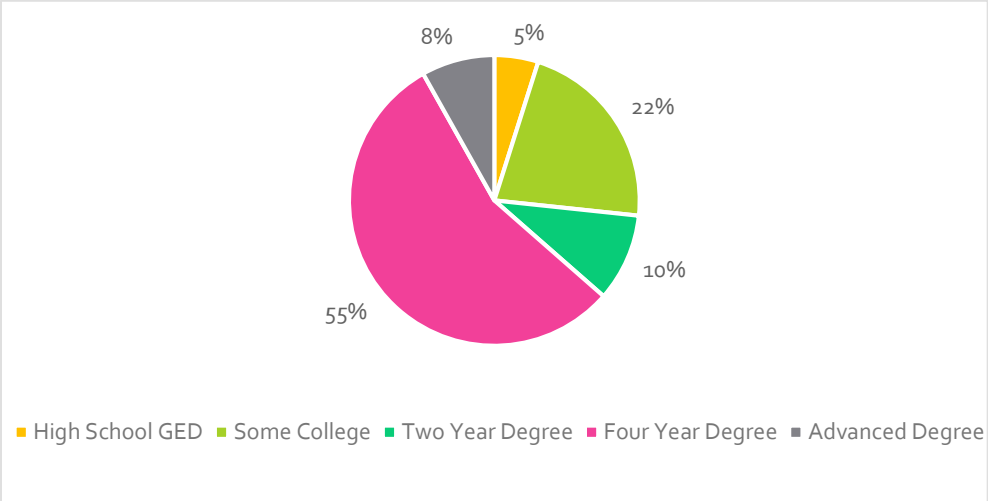


Figure 2.9: Student's t Test Showing the Comparison between Squads A and B at Time 1 to Determine if They Differed on Education

Squad	N	Mean	SD	SEM	t	Results
A	98	3.51	1.048	0.106	1.167	Not Sig.
B	157	3.35	1.091	0.087		

Prior research studies have found that the experience of wearing a BWC increases officers' acceptance of the device (c.f., Gaub, Todak and White, 2018). It was hypothesized that the same effect would be discovered in Fairfax. The following figures present the arithmetic mean for Squad A and Squad B on the variable in question. Time 1 refers to the survey administrated prior to the officers knowing if they would be wearing a BWC. Time 2 refers to the survey administered at the end of the pilot.

Figure 2.10 presents the findings concerning the acceptance of BWCs by the respondents to this survey. The variable of acceptance was created by combining the responses to two of the questions on the officer survey focusing upon BWC acceptance.[3] A Student's t Test was performed to determine if Squad A differed from Squad B on acceptance prior to their knowing if they would be the squad assigned them. The test shows that Squads A and B do not significantly differ on their level of acceptance at Time 1 (t = 1.151). A second test was performed to see if Squad A and B differed on levels of acceptance after the pilot program was over (Time 2). The test shows that there is a significant difference between Squads A and B (t = -2.599). One might rush to conclude that what was found in past studies was also found in Fairfax. However, it was decided to drill deeper into this relationship by comparing Squads A and B between Times 1 and 2. Figure 2.10 shows that when comparing each squad between their Time 1 and 2 responses, Squad B slightly increased their acceptance but not to a significant degree. However, when comparing Time 1 and 2 responses for Squad A, the difference was negative and significant. Thus, the differences found in Time 2 comparisons were not due primarily to an increase in acceptance by the

[3] See questions 28 and 29 in the Fairfax County Police Officer Survey in Appendix D

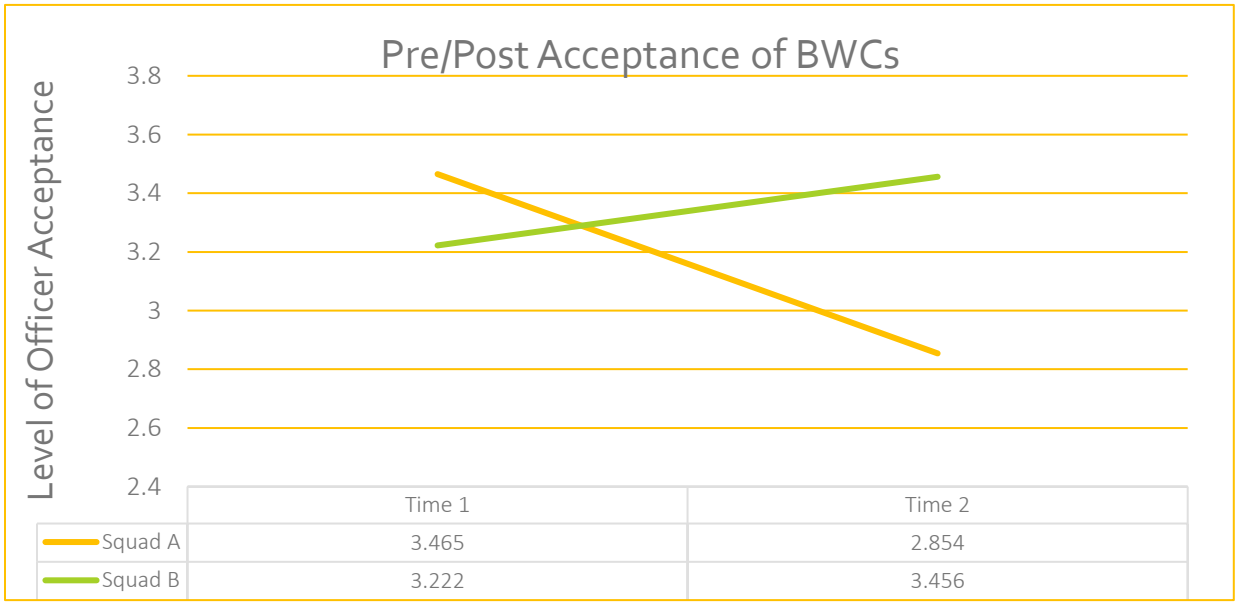
camera-wearing Squad B but by the drop in acceptance by respondents in Squad A. These relationships are graphically displayed in Figure 2.11. One explanation for this unusual finding is that Squad B accepted the BWCs because they were ordered to do so and thus did not change their attitudes concerning acceptance between Time 1 and 2. Some officers in Squad A, however, may have heard that the use of the cameras required more work on the officer's part such as "tagging the incidents" which might explain their negative response to acceptance at Time 2.

Figure 2.10: Student's t-Tests between Squad A and Squad B Officers and between Their Responses between Time One and Two

Squad	Mean T1	SD T1	Mean T2	SD T2	Btn A_1 & B_1	Btn T_1 & T_2	Btn. A_2 & B_2
A	3.465	1.650	2.854	1.588	1.151	-2.694*	-2.599*
B	3.222	1.693	3.456	1.747		1.003	

* = p. < .05

Figure 2.11: Changes in Acceptance Levels of BWCs Over Time



Content Area 1: BWC's Effect on Citizen Behavior

Six statements were presented in this area and the officers were asked to respond to each statement by selecting one of seven response categories ranging from strongly disagree to strongly agree.[4] The seven categories were collapsed into three to make the resulting figures more interpretable. The figures present responses to a statement divided by whether the respondent was a member of Squad A or B and

[4] To conserve space only two of the statements will be presented. The two presented are considered the most important of the statements in this area.

then further subdivided by time: responses prior to knowing if they would wear the camera and after the end of the pilot program.

Figure 2.12 presents the respondents' belief about whether the BWCs will increase police-community relations. At Time 1 and Time 2, the majority of Squad B officers disagreed with the statement that BWCs will improve relations. However, there was a slight increase in agreement across time in Squad B's responses to the statement (13% to 24% agreement). Squad A's agree response decreased slightly over time (17% to 15%). A Chi Square X^2test statistic was calculated for the response category of agree across squad and time. For data in Figure 2.12, the X^2 value is 2.256 and the *p* value is .133 which is not significant at the .05 probability level. Thus, there is no significant difference across percent agree with the statement that BWCs will improve community relations by squad and time.

Figure 2.12: BWCs Will Improve Police Community Relations, by Squad and Time

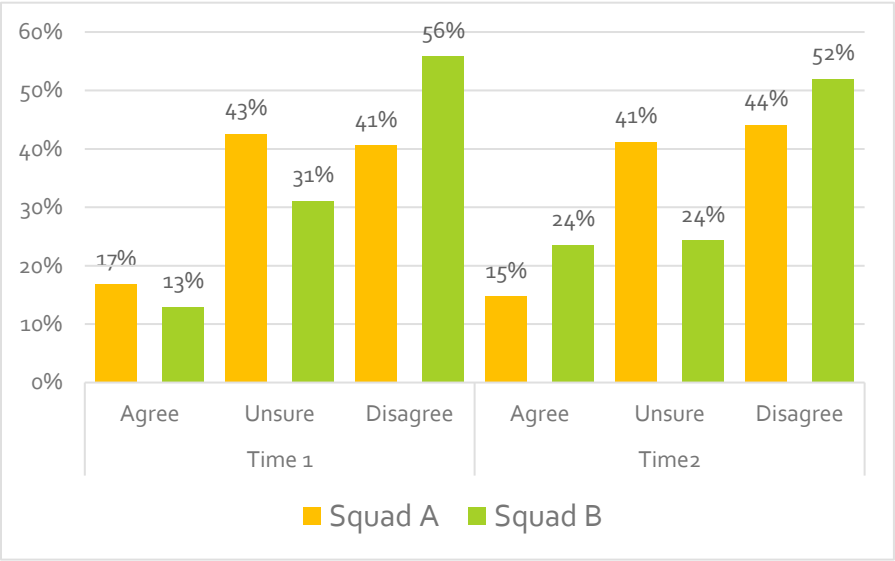
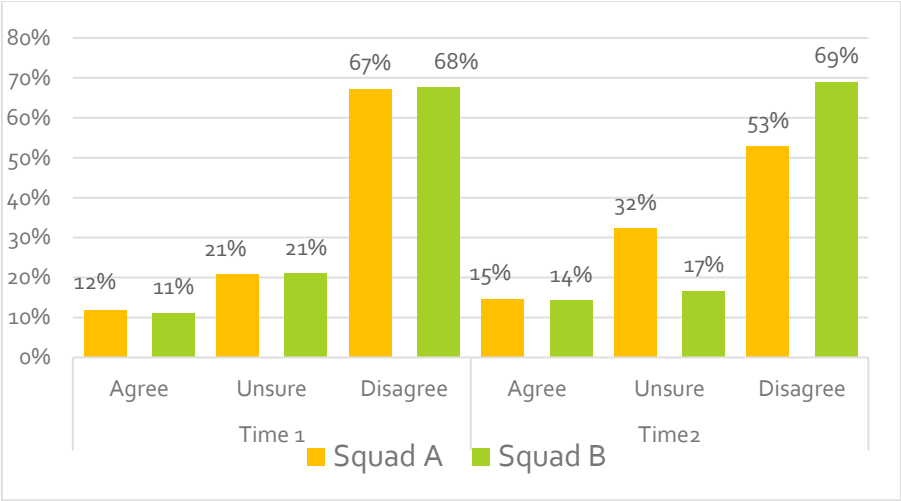


Figure 2.13 shows that both squads strongly disagree with the statement that BWCs will improve police legitimacy in the eyes of the community at time one (67% and 68%). Squad B maintains its disagreement at time two while Squad A disagrees less and shifts that response to the unsure category. Both squads agree responses are similar over time with Squad A being 1% higher. In short, neither Squad A nor B respondents feel that the BWC will have any effect on the public's perception of police legitimacy. A Chi Square test statistic is calculated for the response category of agree across squad and time. For data in Figure 2.13, the X^2 value is .061 and the *p* value is .805 which is not significant at the .05 level. Thus, there is no significant difference across percent agree with the statement that BWCs will increase legitimacy by squad and time.

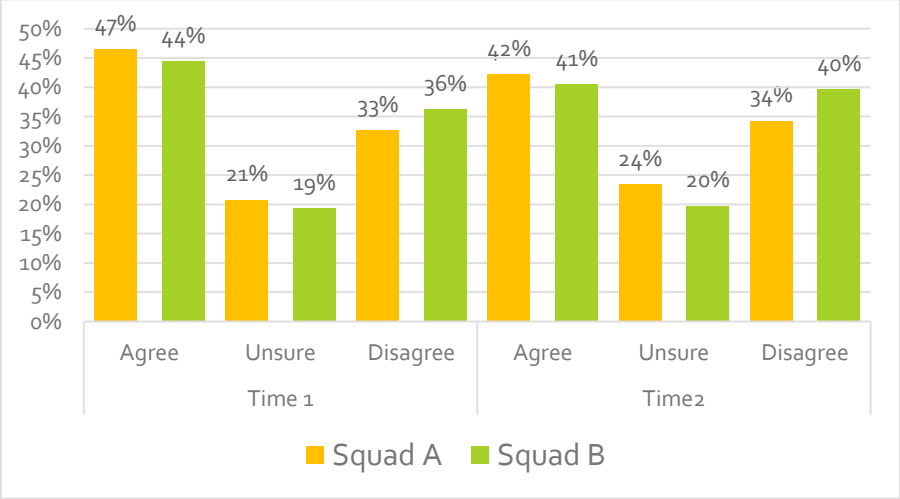
Figure 2.13: BWCs Will Improve Police Legitimacy Among Community Members, by Squad and Time



Content Area 2: BWC's Effect on Police Officer Behavior

This section addressed the question as to whether the BWCs will affect police officers' behavior. Again, only two of the nine statements will be analyzed for this report. Figure 2.14 asks the respondents to assess whether the BWCs will make the officers act more professionally. The respondents either agree with the statement or disagree at both Time 1 and Time 2; few respondents are unsure. Squad A agrees with the statement slightly more than Squad B (47% to 44% and 42% to 41% at Time 2). A Chi Square test statistic is calculated for the response category of agree across squad and time. For data in Figure 2.14, the X^2 value is .019 and the *p* value is .890, which is not significant at the .05 level. Thus, there is no significant difference across percent agree with the statement that BWCs will increase professionalism by squad and time.

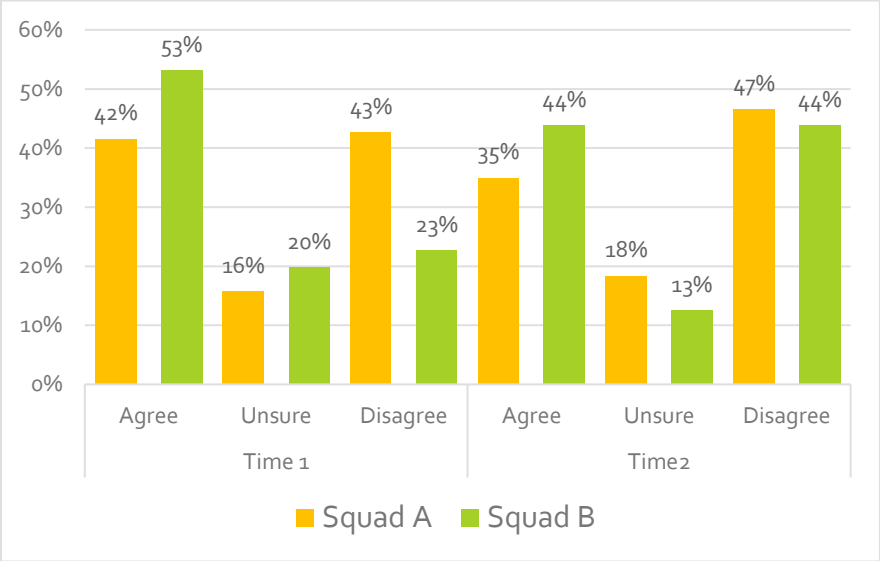
Figure 2.14: BWCs make Police Officers Act More Professionally, by Squad and Time



Another issue that has surfaced in prior research is whether the use of BWCs will reduce the number of proactive police stops. That is, will officers reduce the number of encounters with community members

because they are afraid of having a bad encounter recorded for their supervisors to review? Figure 2.15 presents data that answer that question. Again, the respondents to the statement that BWCs will reduce proactive encounters with community members have polarized responses. The respondents either agree that BWCs would reduce proactive encounters or they disagree with that statement. Both squads decrease their agreement between time 1 and time 2 and increase their disagreement from time 1 tot time 2. A Chi Square test statistic is calculated for the response category of agree across squad and time. For data in Figure 2.15, the Chi^2 value is .019 and the *p* value is .890, which is not significant at the .05 level. Thus, there is no significant difference across percent agree with the statement that BWCs will reduce proactive encounters by squad and time.

Figure 2.15: BWCs Will Reduce Proactive Encounters with Community Members, by Squad and Time



Content Area 3: BWC's Effect on Strength of Evidence

This section addresses the question as to whether the BWCs will affect the strength of evidence used in police work. Again, only two of the four statements will be analyzed for this report. Figure 2.16 asks the respondents to assess whether the BWCs will increase the gathering of evidence. The figure shows that there is overwhelming agreement among the respondents in both Time 1 and 2 that BWCs will increase it. It should be noted that although both squads increase in agreement, the ones wearing the camera (Squad B) increase by more than Squad A (4% points to 17% points, respectively). A Chi Square test statistic is calculated for the response category of agree across squad and time. For data in Figure 2.16, the X^2 value is .482 and the *p* value is .487 which is not significant at the .05 level. Thus, there is no significant difference across percent agree with the statement that BWCs will increase the gathering of evidence by squad and time.

Figure 2.16: BWCs Increase the Gathering of Evidence, by Squad and Time

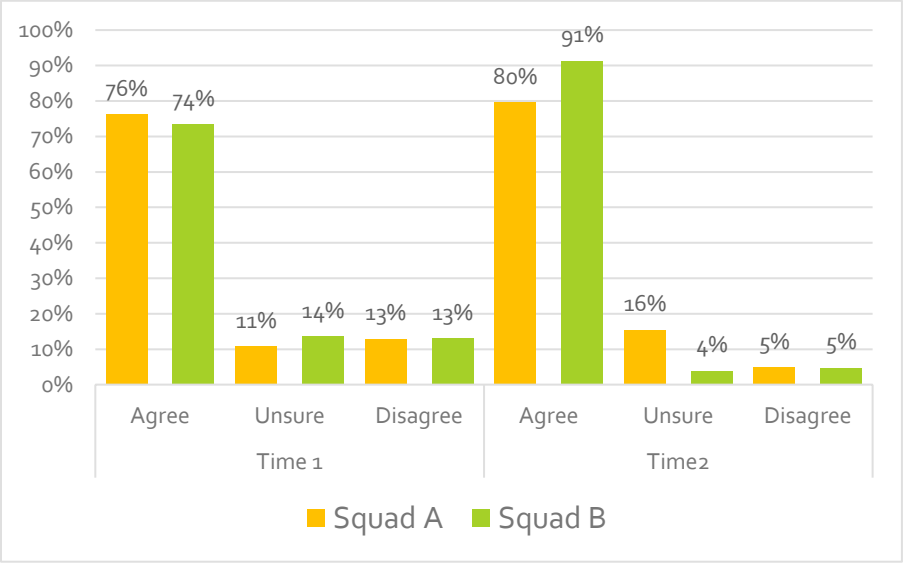
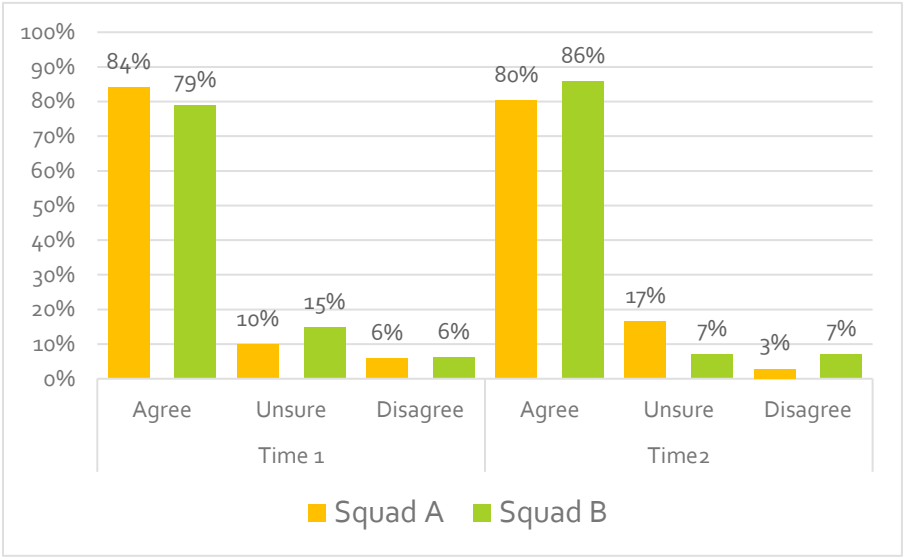


Figure 2.17 shows the officers' responses to the statement on whether BWCs will help in settling complaints against officers. Again, there is overwhelming agreement by members of both Squad A and B to the statement at Time 1 (84% and 79%, respectively). At Time 2, Squad B shows an increase over their response at Time 1 by 7%. However, Squad A showed a reduction in agreement at Time 2 (-4%). A Chi Square test statistic is calculated for the response category of agree across squad and time. For data in Figure 2.17, the X^2 value is .367 and the *p* value is .545 which is not significant at the .05 level. Thus, there is no significant difference across percent agree with the statement that BWCs will help settle complaints by squad and time.

Figure 2.17: BWCs Will Help Settle Complaints Against Police Officers



Content Area 4: Officers' General Perceptions about BWCs

This section addresses the question as to whether BWCs will affect a range of other issues relating to police work. Again, only two of the seven statements will be analyzed for this report. Figure 2.18 displays the responses on whether the use of BWCs will increase officer safety. A majority of both squads indicate that the BWCs will not increase their safety on the street. However, they disagree more at Time 1 than they do at Time 2. The undecided category remained about the same for both groups at both times. A Chi Square test statistic is calculated for the response category of agree across squad and time. For data in Figure 2.18, the X^2 value is .919 and the *p* value is .338 which is not significant at the .05 level. Thus, there is no significant difference across percent agree with the statement that BWCs will increase officer safety by squad and time.

Figure 2.18: BWCs Increase Officer Safety, by Squad and Time

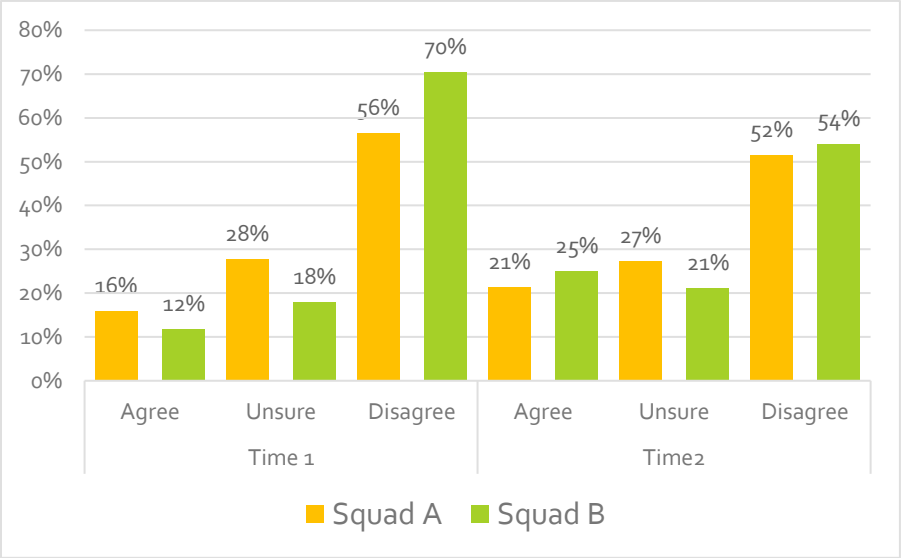
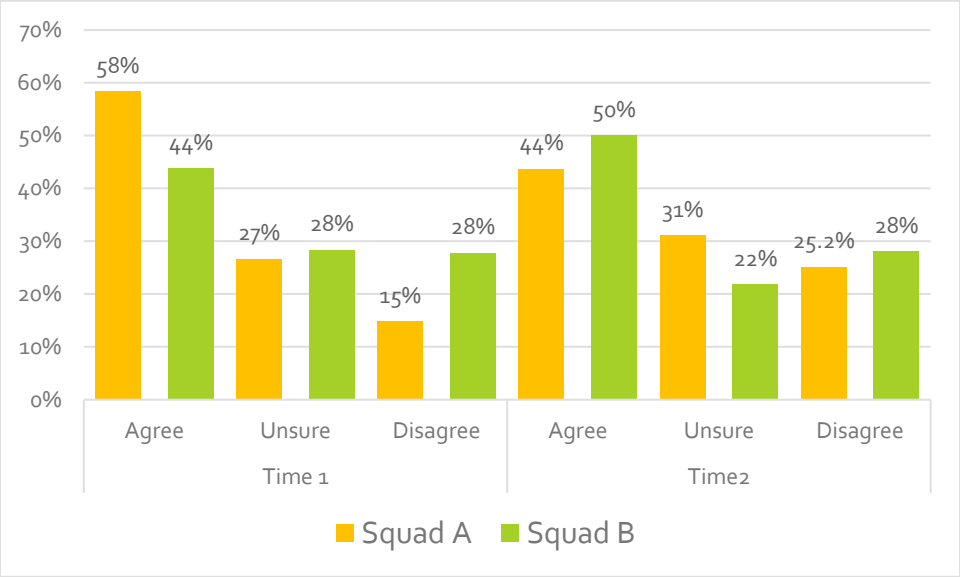


Figure 2.19 shows whether the respondents believe that BWCs will increase the transparency of the department with the public. At Time 1, Squad A is in more agreement with that statement than Squad B (58% to 44%, respectively). However, at Time 2, this relationship reverses, so that Squad B is in more agreement with the statement than Squad A (44% to 50%, respectively). Again, experience with wearing the camera might have strengthened the belief that BWCs will increase the FCPD's transparency to the public. A Chi Square test statistic is calculated for the response category of agree across squad and time. For data in Figure 2.19, the X^2 value is 1.983 and the *p* value is .159 which is not significant at the .05 level. Thus, there is no significant difference across percent agree with the statement that BWCs will increase transparency of the department by squad and time.

Figure 2.19: BWCs Will Increase Transparency of the Department with the Public, by Squad and Time



PART C. FOCUS GROUP METHODOLOGY AND RESULTS

The research team conducted 12 focus groups over the year-long pilot program evaluation. Two groups, one with senior officers and one with line officers, were held in each of the three stations in May 2018 before the pilot began. Six new groups were held following the same design in May 2019 after the pilot ended. All attendees were volunteers and were given a consent form on their rights as participants and verbally agreed to the recording of each session for research purposes. The three focus group moderators used identical guides for the first and second groups.

The first six groups consisted of Squad B officers who were asked for their initial thoughts at three time points: when they learned that the FCPD was considering issuing body-worn cameras, when they learned that their district would be one of only three to participate in the pilot program, and when they learned that Squad B officers like themselves would be issued cameras. The six post-pilot focus groups consisted of Squad A officers who were asked whether they had worn a camera, the extent of their interaction with Squad B officers during the pilot period, and their perceptions regarding whether and how Squad A and Squad B have changed their policing practices because of the cameras.

One rationale for holding separate focus groups for each squad was to give the groups a common frame: all of the participants in a group had used cameras or all of the participants had not. The second rationale was stronger: to hear from each squad independently whether they intermingled while on duty. It was critical to the study's design that only Squad B officers wore BWCs and that community members exposed to BWCs did so only because they engaged with Squad B officers. The researchers learned, after the designation of Squad B as the treatment group, that the two squads occasionally mixed while on duty. In "staff 90" situations, one squad is short-handed and its supervisors ask members of the other squad to serve overtime in order to bring the shift to full staffing. To counter this threat to the integrity of the study design, the department's administration issued a directive to Squad B personnel not to wear their BWCs when they staff 90-ed for Squad A. Never having been assigned a BWC, Squad A officers did not

wear one when they staff 90-ed for Squad B. The focus group uncovered only a few instances in which this directive was not followed.

The 12 recordings or sets of notes from the focus groups were content analyzed to identify the major themes, and then quotes illustrating each theme were selected for this report. The first eight themes listed below were based on comments made by Squad A and Squad B members both before and after the pilot period. The ninth theme consists of other issues deemed important for FCPD to know. Many of the qualitative insights gained from the focus groups are used in this report's interpretation of the quantitative survey results.

1. **Many officers believe that BWCs are needed in police agencies with serious community relations problems, corruption or where egregious law enforcement incidents have occurred; that is not true for FCPD.**

There was mention by participants in almost every focus group that BWCs are most necessary for troubled police agencies facing charges of racism, undue force, etc. Comparisons were drawn to other departments in the Washington DC metropolitan area where BWCs have already been adopted because "they have those problems big-time." When this point was made, it was quickly followed by one or more participants pointing out that FCPD is a highly professional organization without those types of problems.

> *"We don't need it. Ferguson wouldn't happen here."*
>
> *"I don't think we have that type of department where we need a third eye watching us. The majority of officers do their job correctly."*
>
> *"It's a solution to a problem we don't have."*
>
> *"Fairfax County doesn't have a reputation of improper use of force or corruption issues. That's why I chose it."*

2. **Some police officers think that the funding of BWCs means their pay raises will be further delayed.**

Concerns about the funding source for BWCs vied for first mention with comments about the cameras not being needed. Some focus group participants, both pre- and post-pilot, were certain that BWC funds and salary funds reside in the same budget category and would be treated in zero-sum fashion if the decision was made to deploy BWCs to all police officers. One supervisor (see the last quote) referenced efforts to tell officers otherwise.

> *"I don't have a problem with the cameras, but I think the money ought to be spent elsewhere, like on tasers, pay raises, and getting a better fleet of cruisers first."*
>
> *"I first thought BWCs were a ridiculous idea. I thought why are they spending all of that money when they haven't gotten our guys raises in however long?"*
>
> *"When the pilot got close to the end and the question was do we get them or not, the rumor was still growing that if we get cameras, we won't get a raise for 10 years."*
>
> *"We can't seem to [quash] rumors among officers that haven't had a raise in 10 years that the BWC system is coming from a different pool of money and can never be turned into a raise."*

3. There was a general resistance to the BWC pilot program, but it seems to have lessened.

At the beginning of the pilot program, there was some resistance among officers to BWCs unrelated to funding or the department's professionalism. This type of resistance appears to have disappeared over time as officers' gained experience with the technology.

> *"The program raises a concern: Where have I gone wrong? What have I done wrong? You feel violated a bit."*
>
> *"I don't think they've given us enough background on why we need them."*
>
> *"At first I thought it's something more we can get in trouble for by our commanders and supervisors, but actually the only kind of behavior camera-wearing officers are being dinged for are small procedural mistakes like forgetting to tag their recordings appropriately."*
>
> *"The officers given cameras are seeing some of the benefits of them, not only disproving allegations that they would be jammed for trivial mistakes but also seeing in court how the cameras are making their cases stronger."*

4. Most police officers believe that their behavior has not changed because of BWCs.

There was frequent mention of the in-car videos (ICVs) as an earlier version of BWCs, so the officers were already accustomed to having their actions and words recorded, reviewed and used in courtrooms when the BWC pilot was announced.

> *"If anything, I was worried at first about officer hesitation because of Ferguson, etc. It's not really a camera issue but more about the times."*
>
> *"I always felt I was being recorded or observed already. If we're doing the right thing, BWCs won't be a problem."*
>
> *"Every building we go into has cameras all over the place. Everyone's used to it."*
>
> *"We have cameras in our vehicles and mics on our vests and those can pick up a pretty long ways, like in a house. We're very used to being on camera long before we were introduced to BWCs."*
>
> *"The citizens were video and audio recording us long before we were introduced to the cameras."*

5. The officers also believe that community members' behavior hasn't changed because of BWCs.

In nearly every focus group, the officers mentioned the proliferation of public and private recording devices that have shaped the behavior of community members before BWCs were introduced. They also discounted that newly deployed BWCs are even noticed in officer-community member engagements.

> *"The external vests have so many attachments, citizens don't see the camera."*
>
> *"They are oblivious and are going to do what they're going to do."*
>
> *"Ninety-five percent of the people don't know they are being recorded. You give them a card [telling them they are] and they say 'Oh, does my hair look alright?'"*
>
> *"Citizens have been recording officer interactions with their cell phones. Our body-worn cameras don't make a difference."*

"The only advantage to us of the video is its clarity. Everyone thinks we had body cameras already and that's why the camera doesn't change how anyone acts around us."

6. There are positive and negative perceptions of how BWCS have impacted justice system processes, especially the credibility of police officer testimony.

The focus group participants provided an interesting mix of comments on this theme, some focused on the importance of video footage to a case and some lamenting the discounting of their professional testimony.

"Our testimony doesn't mean anything. That's been proven by years of in-car videos. Before then, officers sworn under oath meant something was a fact."

"My word used to be enough. Now if something is not caught on tape, it didn't happen."

"When defense attorneys learn that the officer was wearing a camera, they're quicker to plea bargain with the prosecutors."

"Before, defense attorneys didn't want anything on video. Now if it's not on video, it didn't happen."

7. BWCs are a significant improvement over ICVs but are not perfect.

The step-up in technology is appreciated but brings with it a few new worries.

"An ICV only records what's in front of the cruiser. The BWCs capture more but they fall off in a tussle and sometimes don't work."

"I've had to return to the station several times a day to fix something with it, spending time I'd rather be patrolling."

"The head-mounted or glass-mounted cameras are preferable. Then you're going to be looking at where the danger is."

"I'd prefer a camera positioned closer to my eyes rather than on my chest. I have a lot of traffic stop footage showing car pillars."

"An officer's eyes see more than a BWC camera does. When testifying about a DUI in court, a defense attorney says 'You said the person did, A B and C but the video doesn't show that.'"

8. BWCs create additional work for officers and supervisors.

Participants agreed that the additional work for an officer is minimal, but it's added on to what they see as an already-lengthy checklist of preparations for going on duty. Supervisors commented that their new responsibility for auditing BWC tapes as well as IVC recording would add 30-45 minutes to their heavy work week.

"As an officer, BWCs have added to an extremely long list of about 30 things we have to do before we start our shift. As a supervisor, I've now got five or six more things to do."

"When I found out I wasn't going to get a camera, I was a little bit relieved I didn't have additional administrative responsibility."

"If I didn't have to spend hours [as a supervisor] running audits, I could be out on the street working with the public."

9. Other important points were made by group participants.

"There could be trust issues with confidential informants – is the camera really off?"

"We've used the videos for teaching. They're definitely useful, something I didn't think about at the beginning."

"There's a lot of behind-the-scenes politicking. If the cameras are brought in, it will look like the department chose the community over us."

"I've had a lot of cellphones shoved in my face. I think we should have BWCs. Now that our word is not taken as gold, it's like a third person standing there. It's kind of sad."

"When I would be interacting with citizens, they'd ask where's my BWC. They thought I was some kind of bad cop because I wasn't wearing one."

"Citizens pull out their phones. Once they see we have cameras, they put theirs away. That's been beneficial."

"I found the BWC interesting. I'm happy that I got one, a new challenge to take on."

"Don't come out with a 4 to 6-page general order that's emailed out. Make it simpler. Maybe the people who have to abide by a policy should have a hand in writing it."

PART D. CONCLUSIONS

Similar to past research, a significant difference was observed after the officers used the BWCs during the six-month pilot program. However, contrary to past research, changes in this relationship are not due primarily to officers wearing the cameras becoming more accepting, but rather because those who did not wear BWCs became more negative towards them. Attitudes concerning the effects of wearing the cameras on community members' behavior, the police themselves, evidence usage and general issues were compared by squad and by time. Officers expressed overwhelming agreement on the use of BWCs in gathering evidence and settling complaints. They expressed mixed feelings about whether BWCs will reduce proactive enforcement, make police officers more professional and make the department more transparent to the public. They expressed negative feelings that BWCs will improve community-police relations and increase their safety on the street.

Comments gathered from the 12 focus groups provided insights helpful in interpreting the survey results. A notable number of participants contended that BWCs are needed by departments with serious community relations problems, violent incidents or corruption; none of those things describe the FCPD, so they wondered why BWCs were being piloted. There was a belief among some officers that BWCs and pay raises would be paid for out of the same "pot" in a zero-sum manner. Given the choice, they preferred ("long overdue") raises. Most officers believed their behavior and that of community members did not change because of BWCs. They acknowledged initial resistance to BWCs but said it has decreased with familiarity over time. They believed that BWC recordings have positively and negatively affected justice system operations. They appreciated the improvements BWCs bring compared with in-car videos, recognized the additional work required by staff and the reality that BWCs are not perfect.

Section Three:

Organizational Data on Officer Performance

Section Three: Organizational Data on Officer Performance

SUMMARY OF FINDINGS:

- The implementation of BWCs has no discernable effect on the number of traffic stops conducted or the number of incidents responded to, both non-violent and violent. Thus, de-policing is not apparent when BWCs are deployed.
- The use of BWCs has no discernable effect on the level of citizen complaints during the implementation of the BWCs but does have a significant effect on levels of complaints after the cameras were taken off the street. Those who wore the cameras have fewer complaints than those who did not. However, the effect is quite small.
- The use of BWCs has no discernable effect upon the general use of force, using direct contact force, using indirect contact force or use of force by pointing a firearm.

PART A. METHODOLOGY

This section presents the findings concerning the effect of BWCs on officer behavior. It includes analyses of whether the use of BWCs affect de-policing, complaints against police officers, and finally, the police use of force.

In addition to responding to calls for service, police officers engage in a wide array of proactive activities including community-oriented policing, problem-oriented policing and traffic enforcement. Often, these types of policing activities involve an additional amount of officer discretion, as they require the officer to make decisions about when and how to engage the community. Although little is known about how BWCs may impact proactive policing, some have suggested that by heightening the level of scrutiny or oversight, BWCs may cause officers to de-police, i.e., ; reduce the amount of proactive engagement with the community.[5]

The data for these analyses were supplied by the FCPD. The traffic and incident data were compiled in each district station by their crime analyst. They were received in Microsoft, Excel files. The complaint and use of force data were supplied by the Internal Affairs Bureau of the FCPD. Their data accreditation manager sent the data in Microsoft Excel files.

[5] For a review of the de-policing hypothesis, see Wallace, D., White, M. D., Gaub, J. E., & Todak, N. (2018)

To test the de-policing hypothesis, an interrupted time series regression model examining changes in the weekly seasonal differences in traffic stops was run.[6] The data for the analyses were collected for 12 months before the pilot began, during the six-month pilot and for three months after the pilot ended.[7]

The results of these analyses are found in Figures 3.1, to Figure 3.4 and in Figures 3.1a and b to 3.4a and b. The data were collected 12 months prior to the pilot period to control for possible seasonal differences. The first vertical dotted line in the figures represents the start of the BWC pilot in March 2018 (Week 54). The second vertical dotted line represents the end of the BWC pilot at the end of August 2018 (Week 79). The solid dots refer to the weekly seasonal differences of traffic stops by Squad B. The open dots refer to the weekly seasonal differences of traffic stops by Squad A. The solid horizontal line represents the predicted values for the treatment group (Squad B) and the dashed horizontal line represents the predicted values for the control group (Squad A).

PART B. ANALYSES OF THE PERFORMANCE DATA

Figure 3.1 presents the weekly seasonal differences for traffic stops prior to, during and after the pilot program. A visual scan of the figure shows that there are no differences in the level of traffic stops between Squads A and B. This is confirmed in Figures 3.1a and b, which show that there is no significant difference between the number of traffic stops the two squads made during the implementation period or after the pilot period ended. When reading these figures, look at the fifth column from the left (labeled "p > (t)."). If the values in that column are .05 or less, the change in time is statistically significant. As presented in figures 3.1a and b, neither statistic is significant.[8]

[6] A seasonal weekly difference (subtracting the prior week from the current week) was used since there was a fluctuation in the counts every other week, potentially from the change in schedules across squads. This was done instead of collapsing the data into biweekly aggregates to retain as many timepoints as possible.
[7] Stata software was used to conduct the interrupted timeseries analyses using the "itsa" command (Linden, 2015).
[8] Additional graphics concerning traffic stops, incidents, complaints and use of force can be found in Appendix G.

Figure 3.1: Interrupted Time Series Analysis of BWCs on Traffic Stops

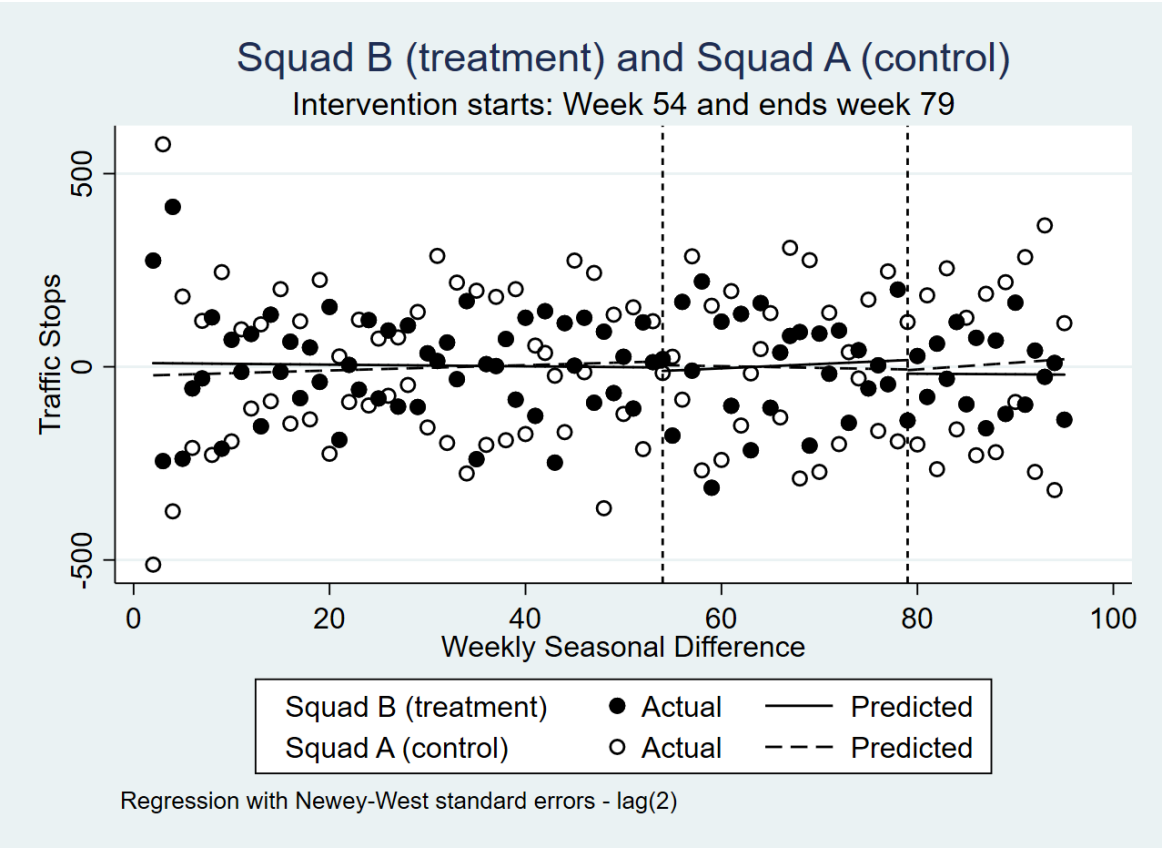


Figure 3.1a: Comparisons of Linear Post Intervention Trends Week 54 to 79

Linear Trend	Coeff.	Std. Err.	t	P>|t|	[95% Conf. Interval]	
Treatment	1.1277	2.7331	0.4126	0.6804	-4.2662	6.5216
Controls	-0.4485	2.8076	-0.1597	0.8733	-5.9894	5.0924
Difference	1.5762	3.9182	0.4023	0.688	-6.1566	9.3089

Figure 3.1b: Comparisons of Linear Post Intervention Trends Week 80 to 94

Linear Trend	Coeff.	Std. Err.	t	P>|t|	[95% Conf. Interval]	
Treatment	-0.1544	3.5644	-0.0433	0.9655	-7.1889	6.88
Controls	1.7696	6.1136	0.2895	0.7726	-10.2959	13.8351
Difference	-1.924	7.0768	-0.2719	0.786	-15.8904	12.0423

Figure 3.2 also presents data that address the issue of de-policing. The data in these analyses are incident data, generated when a police officer responds to resolve an incident. If de-policing was happening because BWCs were deployed, then one should see a decrease in incident activity of Squad B during the pilot period. Again, a visual inspection of the figure indicates that there is no change in Squad B's activity level. Figures 3.2a and b support this finding. The figures show that there is no significant difference

between the number of incidents handled by Squad A or Squad B during the implementation period or after the pilot period ended.

Figure 3.2: Interrupted Time Series Analysis of BWCs on Incidents Responded to by the Police

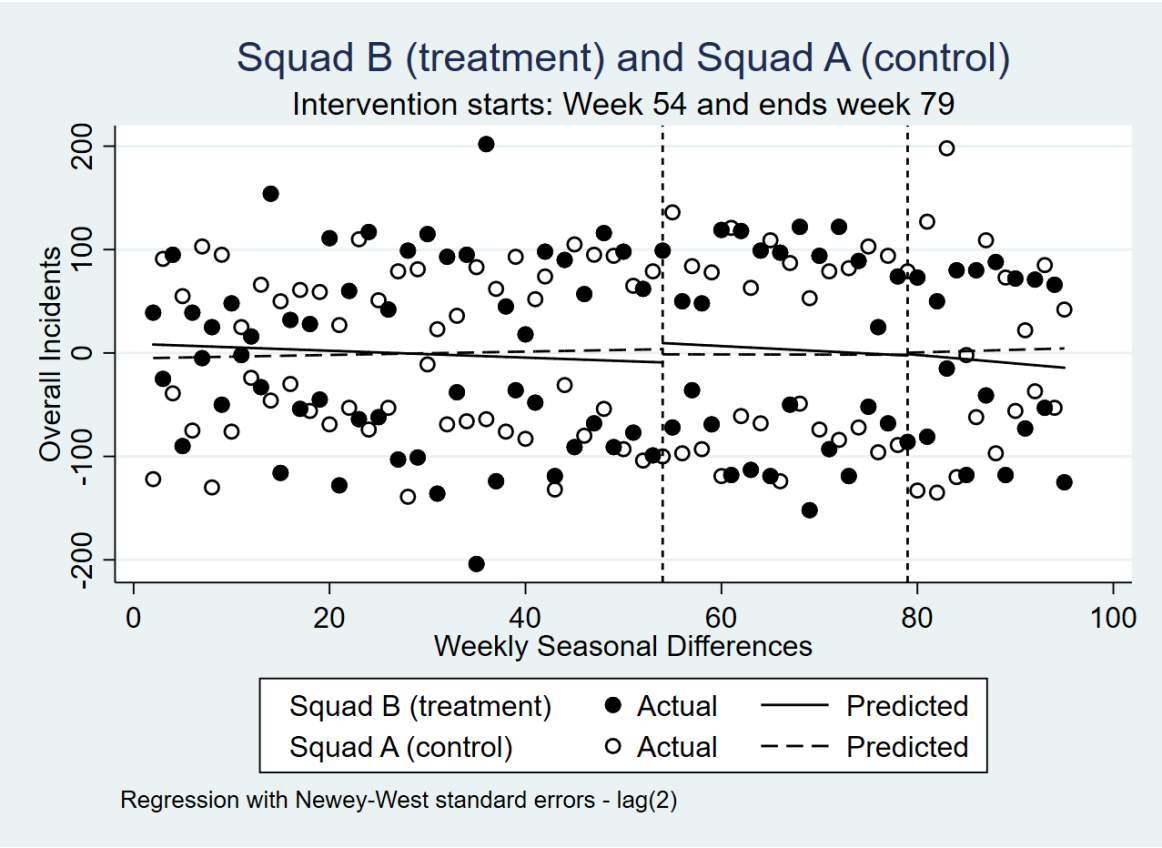


Figure 3.2a: Comparisons of Linear Post Intervention Trends Week 54 to 79

Linear Trend	Coeff.	Std. Err.	t	P>|t|	[95% Conf. Interval]	
Treatment	-0.4823	1.2994	-0.3712	0.711	-3.0468	2.0822
Controls	-0.0146	1.5521	-0.0094	0.9925	-3.0777	3.0485
Difference	-0.4677	2.0242	-0.231	0.8175	-4.4626	3.5272

Figure 3.2b: Comparisons of Linear Post Intervention Trends Week 80 to 94

Linear Trend	Coeff.	Std. Err.	t	P>|t|	[95% Conf. Interval]	
Treatment	-0.8235	2.6606	-0.3095	0.7573	-6.0743	4.4273
Controls	0.2574	2.5827	0.0996	0.9207	-4.8397	5.3544
Difference	-1.0809	3.708	-0.2915	0.771	-8.3987	6.237

When all incidents are analyzed together, there is a chance that different trends in specific incidents might be masking other trends in the data. To investigate this, the incidents were divided into two

categories: non-violent and violent.[9] Figure 3.3 presents the findings concerning non-violent incidents and whether de-policing was evident. That is, did Squad B respond to fewer non-violent incidents during the period that they were wearing BWCs? Again, a visual inspection of the findings indicates that there is no difference between Squad A and Squad B's responsiveness. This finding is supported by data in Figures 3.3a and b. The figures show that there is no significant difference between the number of non-violent incidents handled by Squad A or Squad B during the implementation period or after the pilot period ended.

Figure 3.3: Interrupted Time Series Analysis of BWCs on Non-Violent Incidents Responded to by the Police

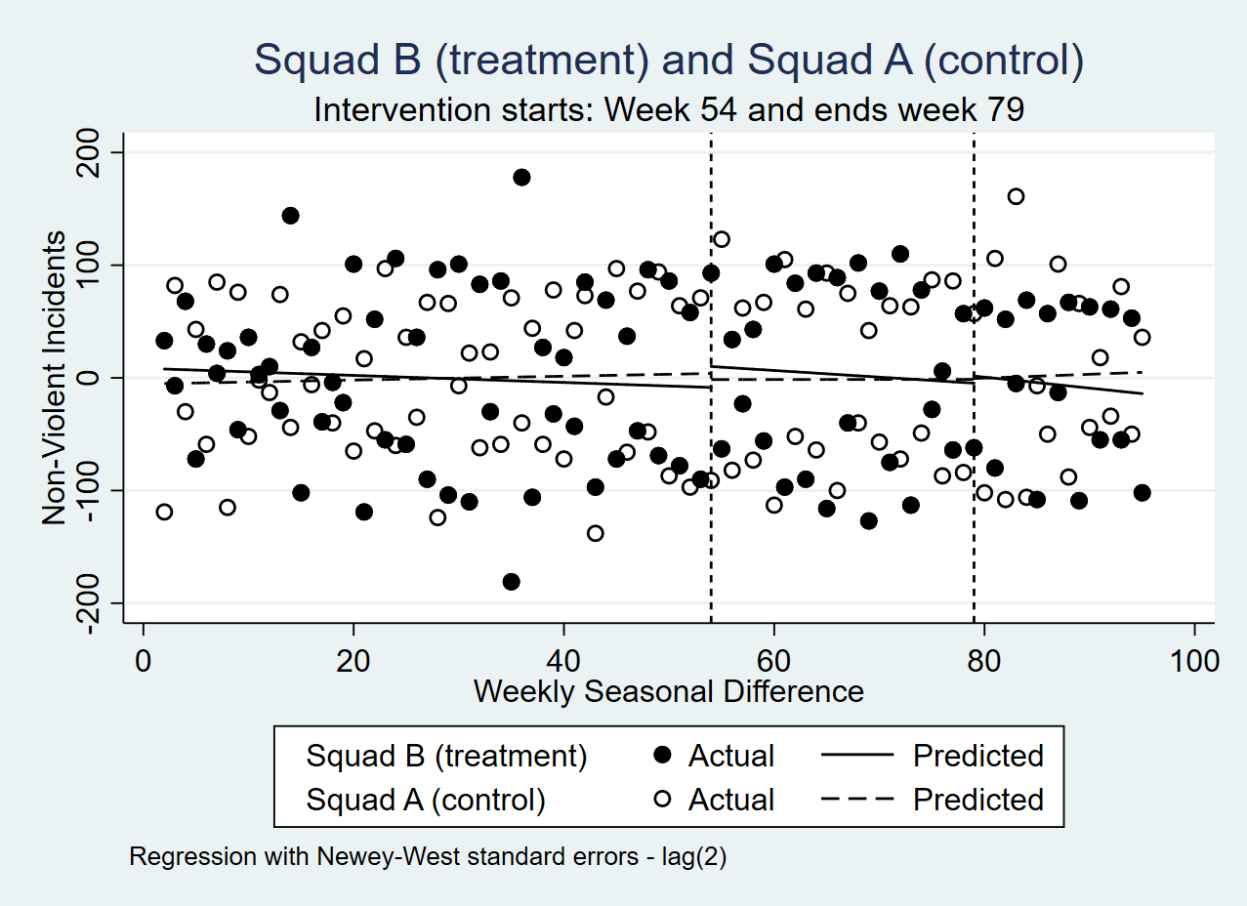


Figure 3.3a: Comparisons of Linear Post Intervention Trends Week 54 to 79

Linear Trend	Coeff.	Std. Err.	t	P>|t|	[95% Conf. Interval]	
Treatment	-0.5908	1.0991	-0.5375	0.5916	-2.76	1.5784
Controls	0.0077	1.3595	0.0057	0.9955	-2.6754	2.6908
Difference	-0.5985	1.7483	-0.3423	0.7325	-4.0487	2.8518

[9] Violent incidents included homicide, assault, kidnapping/abduction, robberies, forcible sex offenses and arson. The non-violent incidents category included all property crimes and those identified as non-reportable.

Figure3.3b: Comparisons of Linear Post Intervention Trends Week 80 to 94

Linear Trend	Coeff.	Std. Err.	t	P>|t|	[95% Conf. Interval]	
Treatment	-0.9755	2.199	-0.4436	0.6579	-5.3154	3.3644
Controls	0.3382	2.0892	0.1619	0.8716	-3.7849	4.4613
Difference	-1.3137	3.0332	-0.4331	0.6655	-7.2999	4.6724

The previous analyses indicated that there is no de-policing for non-violent incidents, but could the effect manifest itself when the incidents are far more serious? Figure 3.4 and supporting data in Figures 3.4a and b present the findings concerning this question. Again, a visual check of the data points indicates that there is no difference between the violent incidents handled by Squad B and Squad A. This finding is supported by data in Figures 3.4a and b. The figures show that there is no significant difference between the number of violent incidents handled by Squad A or Squad B during the implementation period or after the pilot period ended.

Figure 3.4: Interrupted Time Series Analysis of BWCs on Violent Incidents Responded to by the Police

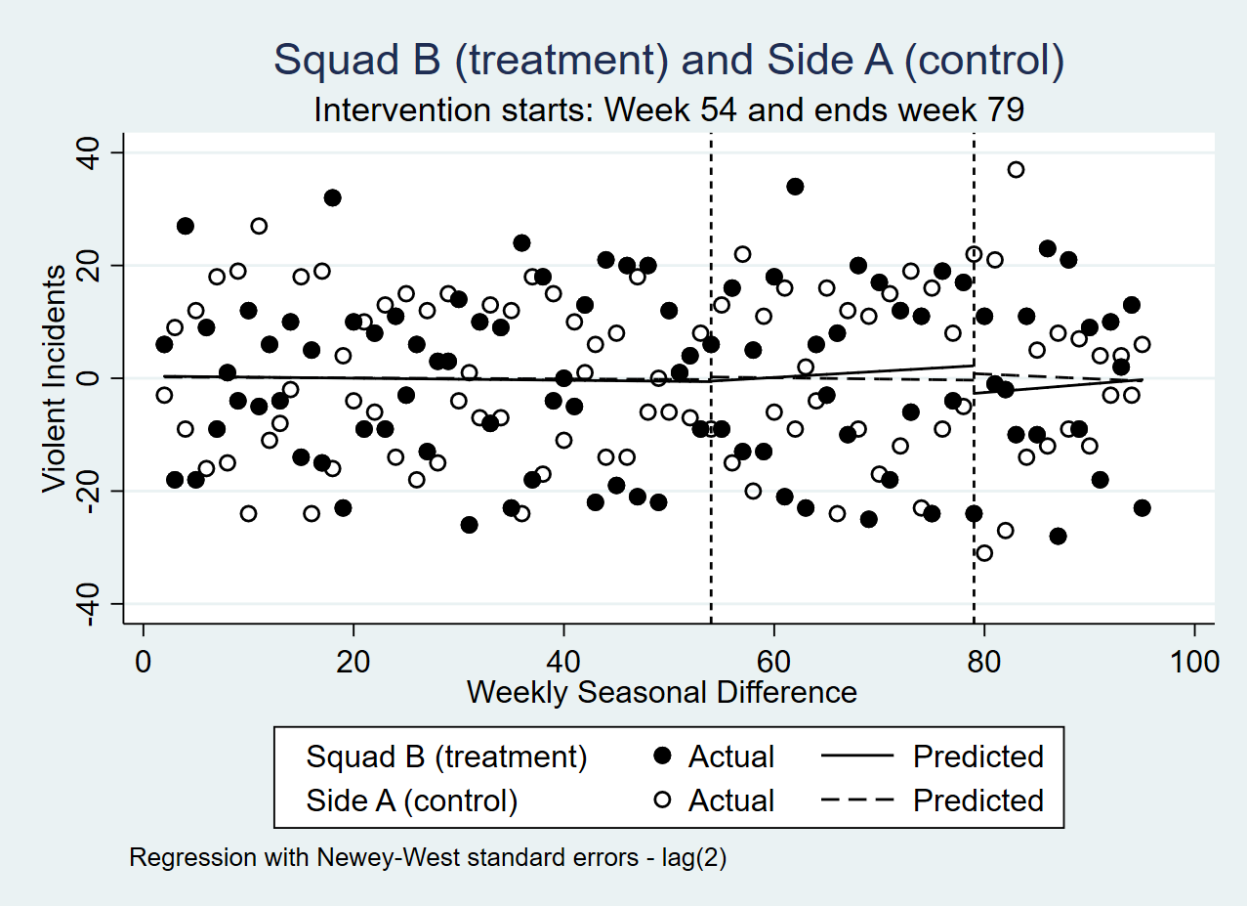


Figure 3.4a: Comparisons of Linear Post Intervention Trends Week 54 to 79

Linear Trend	Coeff.	Std. Err.	t	P>|t|	[95% Conf. Interval]	
Treatment	0.1085	0.2614	0.4149	0.6787	-0.4074	0.6243
Controls	-0.0223	0.2147	-0.1039	0.9174	-0.446	0.4014
Difference	0.1308	0.3383	0.3866	0.6995	-0.5368	0.7983

Figure3.4b: Comparisons of Linear Post Intervention Trends Week 80 to 94

Linear Trend	Coeff.	Std. Err.	t	P>|t|	[95% Conf. Interval]	
Treatment	0.152	0.528	0.2878	0.7739	-0.8902	1.1941
Controls	-0.0809	0.5396	-0.1499	0.881	-1.1458	0.984
Difference	0.2328	0.755	0.3084	0.7581	-1.2571	1.7228

Based upon the preceding four figures and their supporting statistical analyses, one can conclude that there is no indication of de-policing in the FCPD because of the introduction of BWCs.

Next we turn to community complaints. Figure 3.5 presents the findings of the effects of BWCs on community members' complaints against police officers[10]. During the eighteen-month period, only 152 cases were reported.[11] Because, many bi-weekly measuring units had zero complaints, the regression-based analyses can be unstable. The visual assessment of this figure is not as straightforward as the preceding figures. This is due to bi-weekly reporting periods with an outlier number of complaints, then a reporting period with no reports. When the statistical analyses are interpreted, the period running from the beginning to the end of the pilot program shows no meaningful difference in the number of complaints by squad. However, the period after the pilot (weeks 41-47) shows that Squad B had significantly fewer complaints (-.4 complaints per two-week period) while Squad A had more (.2 complaints per two-week period). This difference between the two squads was approximately half a complaint each two-week period. Thus, although the relationships are significantly different, the effect is small.

[10] Caution must be exercised in interpreting these data because the number of complaints is relatively small.

[11] For complaint and use of force data, nine months of pre-pilot data were employed. These data are presented in bi-weekly segments because of the large number of weeks where no complaints were fielded.

Figure 3.5: Interrupted Time Series Analysis of BWCs on Community Member's Complaints on Police Officers

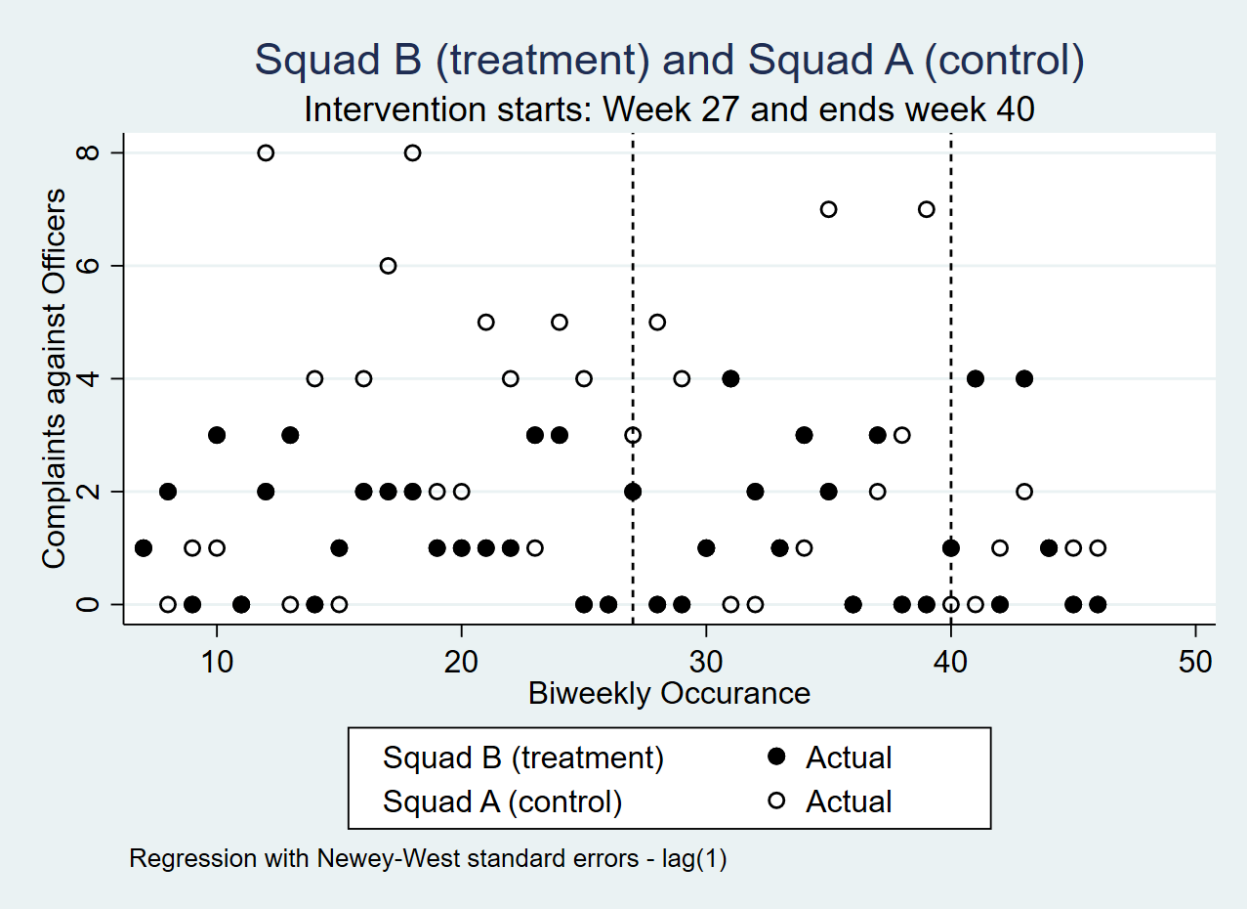


Figure 3.5.a: Comparisons of Linear Post Intervention Trends Bi-weekly 27 to 40

Linear Trends	Coeff.	Std. Err.	t	P>|t|	[95% Conf. Interval]	
Treatment	-0.033	0.1016	-0.3245	0.7465	-0.2357	0.1697
Controls	0.0989	0.202	0.4896	0.626	-0.3042	0.502
Difference	-0.1319	0.2261	-0.5832	0.5617	-0.5831	0.3193

Figure3.5b: Comparisons of Linear Post Intervention Trends Bi-weekly 41 to 47

Linear Trend	Coeff.	Std. Err.	t	P>|t|	[95% Conf. Interval]	
Treatment	-0.3571	0.1676	**-2.1312**	**0.0367**	-0.6915	-0.0227
Controls	0.1786	0.0846	**2.1106**	**0.0385**	0.0097	0.3474
Difference	-0.5357	0.1877	**-2.8537**	**0.0057**	-0.9103	-0.1611

Figure 3.6 presents the interrupted times series findings on the effect of BWCs on the use of force in general. A visual scan of the data points shows two things. First, as one would expect using data representing a rare event, there are outliers in the data set. There were only 610 cases of use of force over

the 18 months of data collection. Second, there doesn't appear to be a distinct pattern for either Squad A or B. Relying on the statistics presented in Figures 3.6a and b, it can be concluded that there is no statistically significant difference either during the pilot period or after (all *p*-values are greater than .05).

Figure 3.6: Interrupted Time Series Analysis of BWCs on Use of Force

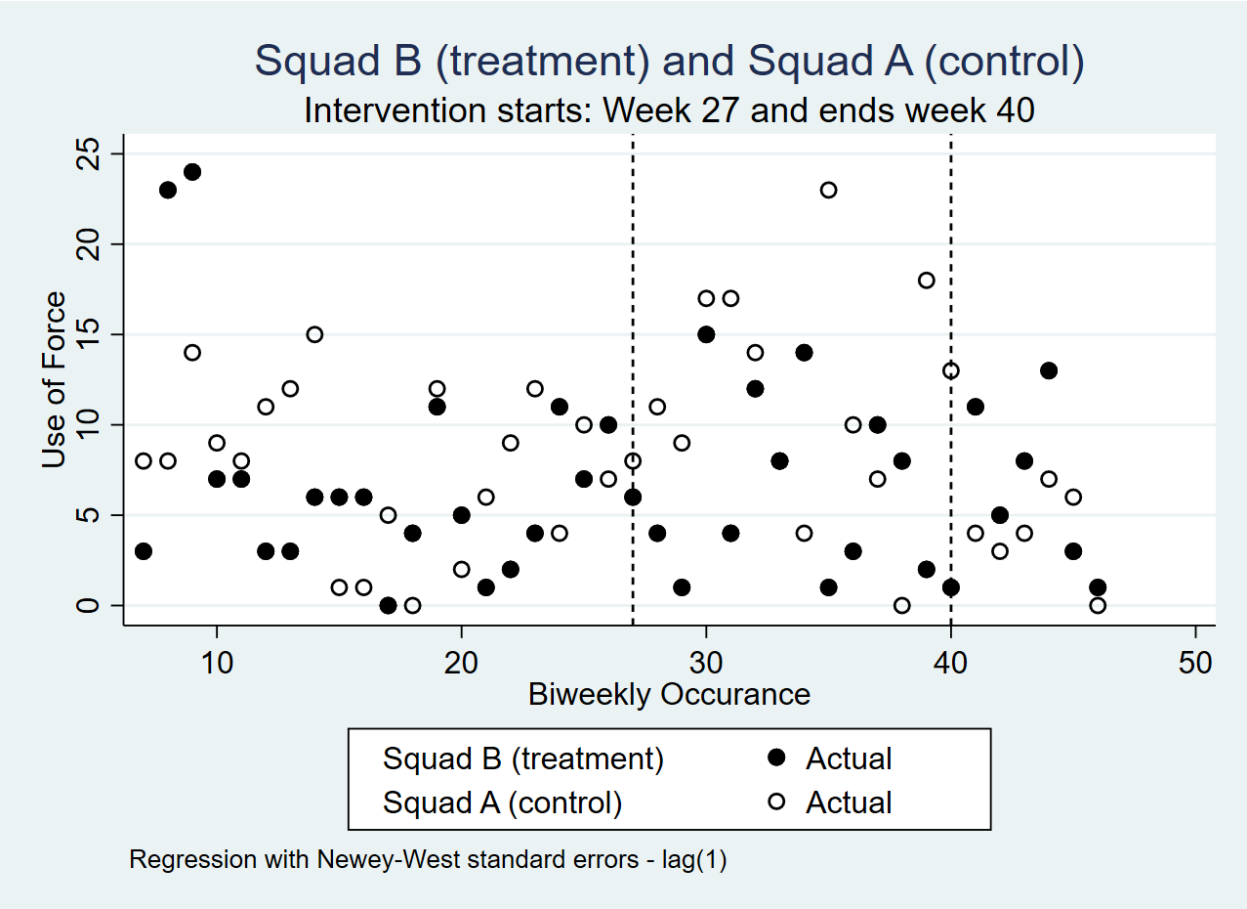


Figure 3.6a: Comparisons of Linear Post Intervention Trends Bi-weekly 27 to 40

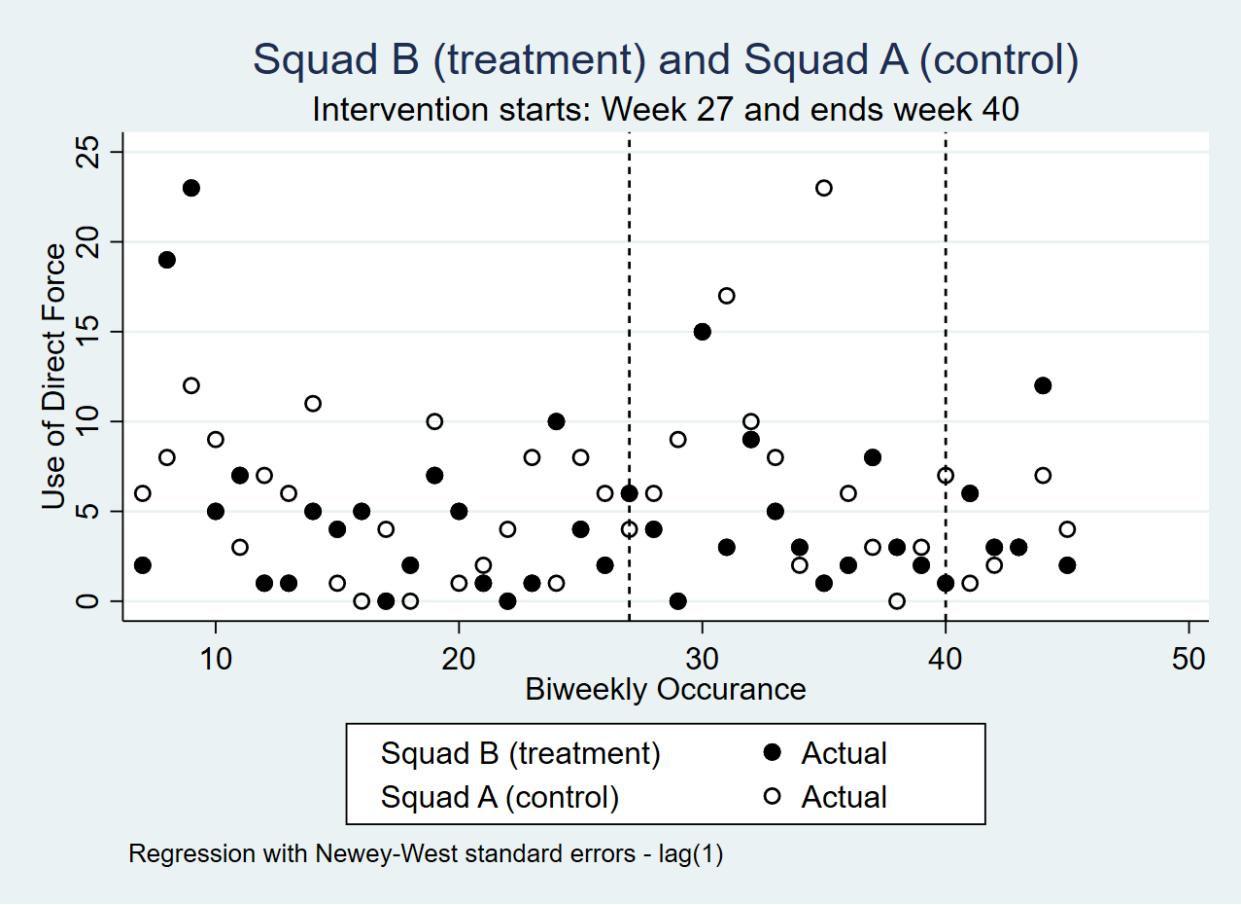
Linear Trend	Coeff.	Std. Err.	t	P>|t|	[95% Conf. Interval]	
Treatment	-0.044	0.2823	-0.1557	0.8767	-0.6074	0.5195
Controls	-0.1209	0.4291	-0.2817	0.779	-0.9772	0.7354
Difference	0.0769	0.5137	0.1497	0.8814	-0.9481	1.102

Figure3.6b: Comparisons of Linear Post Intervention Trends Bi-weekly 41 to 47

Linear Trend	Coeff.	Std. Err.	t	P>|t|	[95% Conf. Interval]	
Treatment	-0.044	0.2823	-0.1557	0.8767	-0.6074	0.5195
Controls	-0.1209	0.4291	-0.2817	0.779	-0.9772	0.7354
Difference	0.0769	0.5137	0.1497	0.8814	-0.9481	1.102

Again, when all use of force incidents are analyzed together there is a chance that different trends in specific incidents of force might be masking other trends in the data. Figure 3.7 presents an interrupted time series analyses on the effect of BWCs on the direct force.[12] A visual scan of the data points shows no distinct pattern for either Squad A or B. Again, relying on the statistics presented in Figures 3.7a and b, it can be concluded that there is no statistically significant difference either during the pilot period or after (all *p*-values are greater than .05).

Figure 3.7: Interrupted Time Series Analysis of BWCs on Use of Direct Contact Force



[12] Types of force were separated into three categories for analysis: direct contact, indirect contact, and pointed firearm. ***Direct contact*** includes: ASP/Baton, Force to Cuff, Force to Hobble, Force to Hold/Restrict, Hands-On Escort/Guide, Pressure Points by Hand, Spit Mask, Strike with Foot/Knee, Strike with Hand/Fist, and Take Down. ***Indirect contact*** includes: Pointed Taser, Taser, Lit with Taser, OC, PIT, and Intentional Vehicle Contact. ***Pointed firearm*** contained only the pointed firearm force type. No incidents of deadly force were reported during the time period of this study.

Figure 3.7a: Comparisons of Linear Post Intervention Trends Bi-weekly 27 to 40

Linear Trend	Coeff.	Std. Err.	t	P>|t|	[95% Conf. Interval]	
Treatment	0.0659	0.063	1.0464	0.2991	-0.0598	0.1917
Controls	-0.0165	0.1132	-0.1456	0.8846	-0.2423	0.2094
Difference	0.0824	0.1295	0.6362	0.5268	-0.1761	0.3409

Figure 3.7b: Comparisons of Linear Post Intervention Trends Bi-weekly 41 to 47

Linear Trend	Coeff.	Std. Err.	t	P>|t|	[95% Conf. Interval]	
Treatment	0.0357	0.0952	0.3753	0.7086	-0.1542	0.2256
Controls	-0.3214	0.1693	-1.8988	0.0618	-0.6592	0.0164
Difference	0.3571	0.1942	1.839	0.0703	-0.0304	0.7447

Figure 3.8 presents the findings of an interrupted time series analyses of the effect of BWCs on incidents of indirect contact force. Here the biweekly data points appear to form a predictable chain across time and between Squads A and B. Reliance upon the statistical analyses is more critical here because of the lack of a clearly visual pattern. Figures 3.8a and b indicate that the difference between Squad B and Squad A are not statistically significant.

Figure 3.8: Interrupted Time Series Analysis of BWCs on Use of Indirect Contact Force

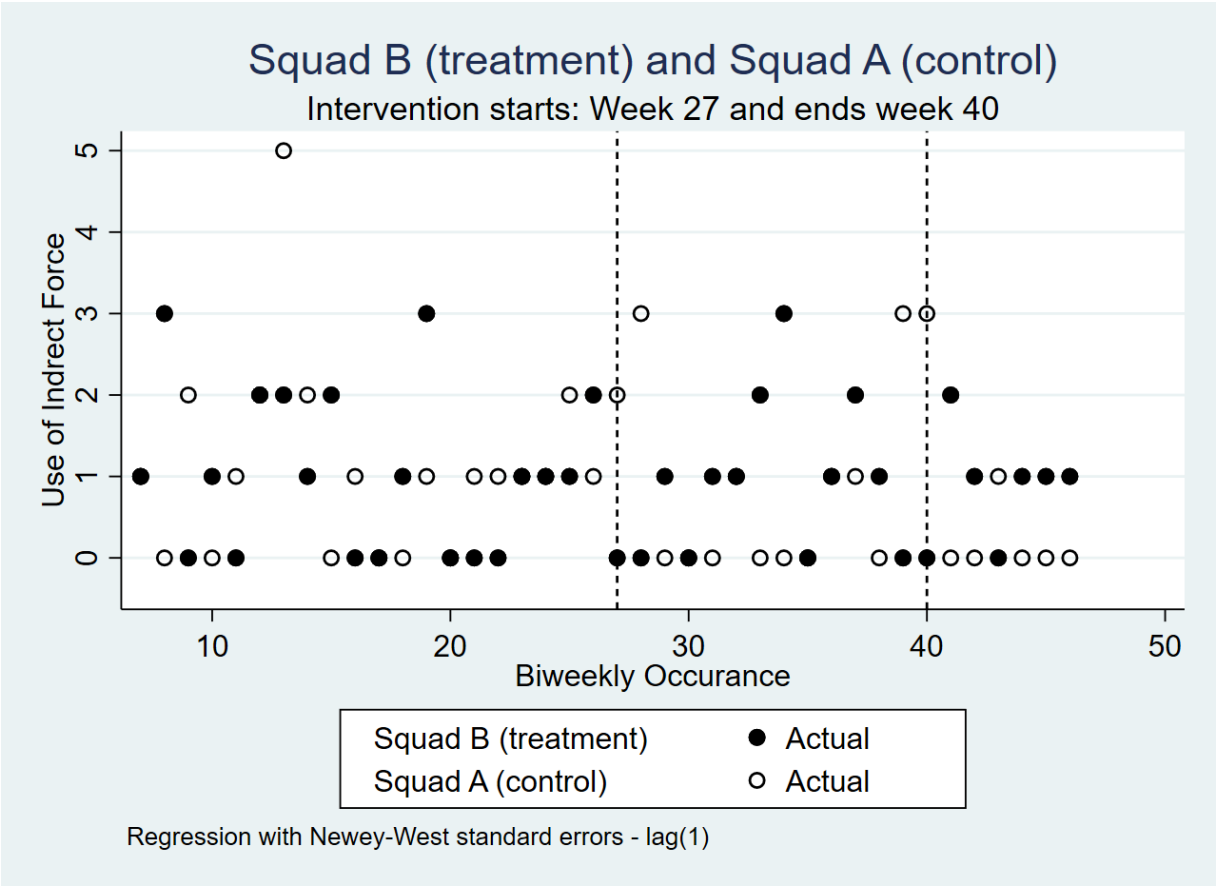


Figure 3.8a: Comparisons of Linear Post Intervention Trends Bi-weekly 27 to 40

Linear Trend	Coeff.	Std. Err.	t	P>|t|	[95% Conf. Interval]	
Treatment	0.0659	0.063	1.0464	0.2991	-0.0598	0.1917
Controls	-0.0165	0.1132	-0.1456	0.8846	-0.2423	0.2094
Difference	0.0824	0.1295	0.6362	0.5268	-0.1761	0.3409

Figure 3.8b: Comparisons of Linear Post Intervention Trends Bi-weekly 41 to 47

Linear Trends	Coeff.	Std. Err.	t	P>|t|	[95% Conf. Interval]	
Treatment	0.0357	0.0952	0.3753	0.7086	-0.1542	0.2256
Controls	-0.3214	0.1693	-1.8988	0.0618	-0.6592	0.0164
Difference	0.3571	0.1942	1.839	0.0703	-0.0304	0.7447

Finally, Figure 3.9 shows the effect of BWCs on the use of force defined as pointing a firearm. This use of force is the one most often reported. About one in six reports on the use of force refers to the force category of pointing a firearm. The pattern of this use visually appears to be constant across time with only a few outliers. Most of these outliers occur during the fielding of the BWCs. Once again, the

statistical analyses must be used to determine if the wearing of a BWC affected the rate of pointing a firearm. Referring to Figures 3.9a and b, neither the implementation phase of the project nor the period following implementation shows a significant difference between members of Squad B or Squad A on the use of force by pointing a firearm. Given this finding, it can be concluded that BWCs do not have a meaningful effect on this category of the use of force.

Figure 3.9 Interrupted Time Series Analysis of BWCs on Use of Force: Pointing a Firearm

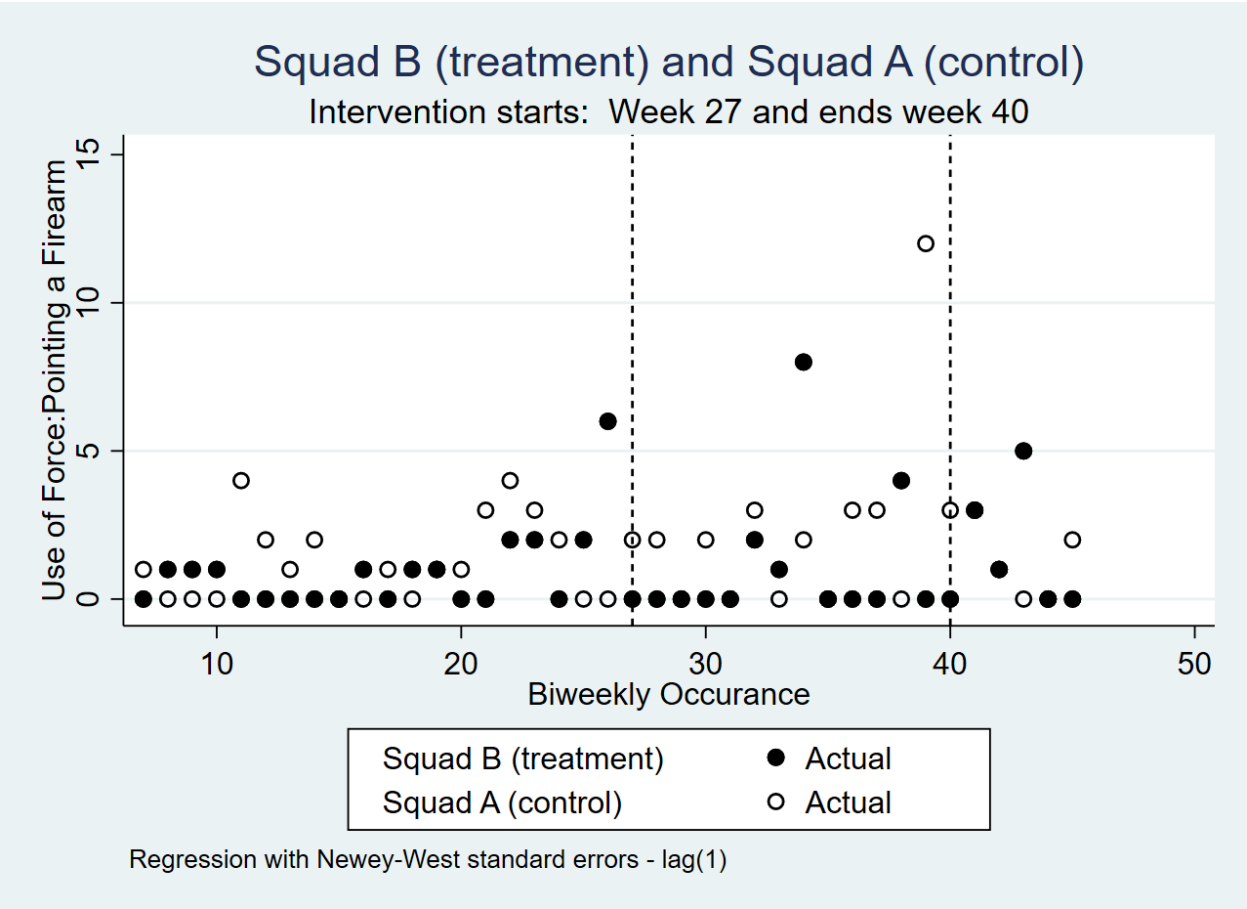


Figure 3.9a: Comparisons of Linear Post Intervention Trends Bi-weekly 27 to 40

Linear Trend	Coeff.	Std. Err.	t	P>|t|	[95% Conf. Interval]	
Treatment	0.1429	0.0937	1.5253	0.132	-0.0441	0.3299
Controls	0.3516	0.2639	1.3327	0.1872	-0.1752	0.8785
Difference	-0.2088	0.28	-0.7457	0.4585	-0.7678	0.3502

Figure 3.9b: Comparisons of Linear Post Intervention Trends Bi-weekly 41 to 47

Linear Trend	Coeff.	Std. Err.	t	P>|t|	[95% Conf. Interval]	
Treated	-0.1429	0.3596	-0.3973	0.6924	-0.8607	0.575
Controls	-0.4286	0.2553	-1.6786	0.098	-0.9383	0.0812
Difference	0.2857	0.441	0.6479	0.5193	-0.5947	1.1662

PART C. CONCLUSIONS

Officer performance data were gathered from the department's own records concerning the number of traffic stops, other incidents, citizen complaints and use of force reports documented before, during and after the pilot period. Based upon the first four figures and their supporting statistical analyses, one can conclude that there is no indication of de-policing in the FCPD after the implementation of BWCs. Concerns about de-policing after the inclusion of BWCs is directly connected to concerns about officer productivity and public safety, however both Squad A and Squad B continued normal operations in making traffic stops and responding to both violent and non-violent incidents during the study.

No statically significant differences are found between squads on levels of complaints during the pilot period of the analyses. However, statistical significance is found in the level of community members' complaints during the post intervention period. Based upon these results, the removal of BWCs from the field is correlated with a 0.4 bi-weekly decline in the average number of complaints for those previously equipped with BWCs. There was an average increase of 0.2 complaints per two-week time period for the control group. The difference in the change in the number of complaints after the removal of BWCs between the squads was statistically significant. However, these effects are minimal and based on a small number of complaints.

No statistically significant differences were found in use of force incidents during the BWC period or following the removal of BWCs from the FCPD officers. Based upon this, BWC usage does not affect use of force in general, direct force, indirect force or use of force by pointing a firearm.

SECTION FOUR:

Perspectives of Community Members

Section Four: Perspectives of Community Members

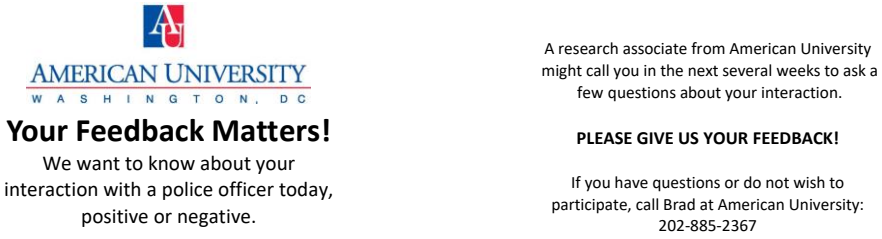
SUMMARY OF FINDINGS

- Community members in the three pilot districts were asked a series of questions regarding a specific interaction they recently had with a police officer and were then asked to agree or disagree with three statements about it:
    - I am satisfied with how I was treated by the officer (83% agree).
    - I am happy with how my situation was resolved (74% agree).
    - I was treated in a procedurally just manner, i.e., with respect, fairness, professionalism, and the officer listened and explained actions and decisions (92% agree).
- On all three questions, substantially higher percentages of older respondents agree than did younger respondents.
- On all three questions, substantially higher percentages of Caucasian and Asian respondents agree than did African Americans, Hispanics and Native Americans.
- On all three questions, the levels of agreement by men and women are virtually identical.
- The community members were also given two statements about the FCPD:
    - The FCPD does its job well (84% agree).
    - The FCPD shares the values of my community (81% agree).
- Responses showed the same pattern of support by age group and race/ethnicity as above.
- The final statement asserted that BWCs should be worn by all officers in the department (92% agree).
- Community members were asked whether the officer was wearing a BWC and approximately one-third accurately responded yes or no, while two-thirds responded incorrectly or said they are unsure.
- The status of the officer as either wearing a BWC or not did not affect responses to any of the six statements listed above.
- In sum, there is widespread support for the actions of FCPD officers and the department itself in the attitudes of community members with recent police interactions, even though some age and racial/ethnic groups are less positive than others.
- The support for the adoption of BWCs department-wide is very strong.

PART A. SURVEY METHODOLOGY

In preparation for the telephone survey, cards were printed and given to the police officers in the three participating districts to hand to community members with whom they would come in contact for the duration of the pilot period. The cards were the size of a typical business card and told the recipient to anticipate a call from the American University research team. The front and back sides are shown in Figure 4.1.

Figure 4.1: The Survey Recruitment Card Handed out by Officers

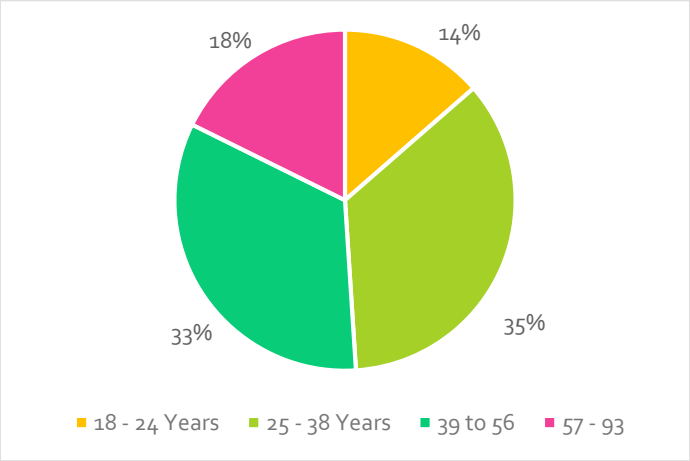


An FCPD district crime analyst provided the research team with a list of those community members that had an encounter with a police officer within the prior two weeks. The list included only the first name of the community member, the phone number they gave the police, whether the officer was wearing a camera or not and the date of the incident. Students from American University who spoke English as well as Spanish, Korean or Vietnamese (the four most spoken languages in the district's communities) were recruited and trained as interviewers to conduct the telephone surveys. The survey questions were programmed into a software program (Qualtrics) that automated question flow, skip patterns, and the input of responses to open-ended questions. A total of 603 community members were interviewed, producing a response rate of 19.5% from all people whose first name and phone number were relayed. In addition, during the interview period, there was a dramatic increase in spam calls in the area.[13] This external condition may have reduced the number of calls answered by community members during the survey period.

PART B. ANALYSES OF THE SURVEY DATA

Figures 4.2 through 4.4 present the demographics of the sample of community members by age, gender and race/ethnicity.[14] As shown in Figure 4.2, the majority of survey respondents (68%) are in the 25 to 56 years category. Lesser percentages are between 18 to 24 years (14%) and over 57 (18%).

Figure 4.2: Age of Respondents

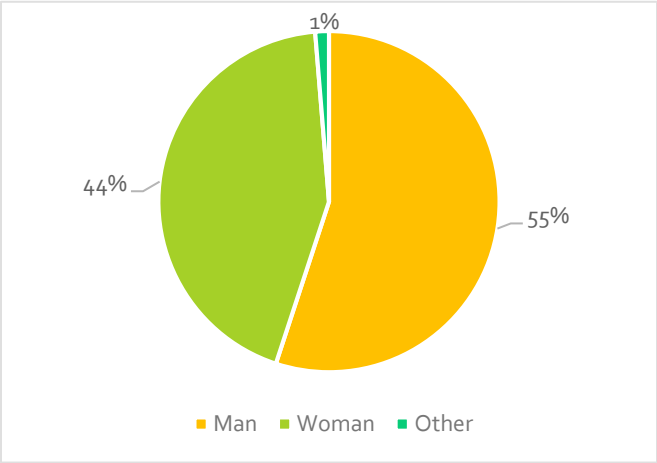


[13] For example, see https://wjla.com/news/local/virginia-lawmakers-want-to-stop-spoofed-robocalls

[14] The survey was administered by phone and in four of the most widely spoken languages in the Fairfax County: English, Spanish, Korean and Vietnamese.

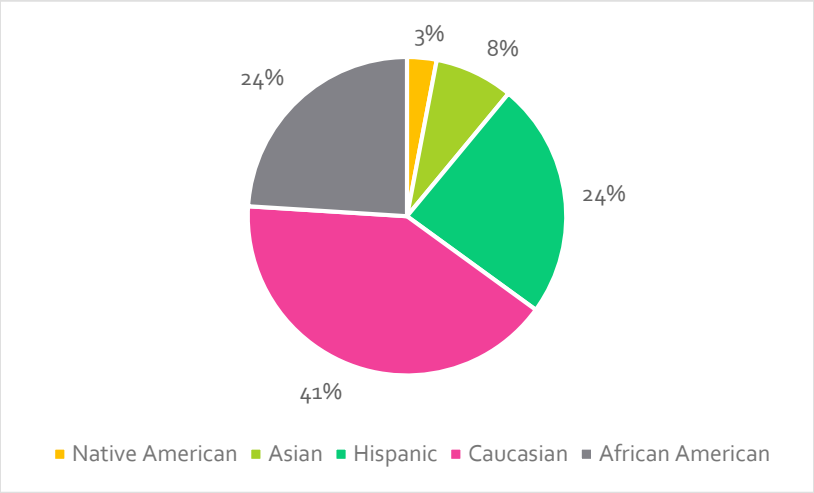
Men composed the majority of the respondents (55%) and women composed 44% (see Figure 4.3). One percent of the respondents identified themselves as other than man or woman.[15]

Figure 4.3: Gender of Respondents



Respondents' race/ethnicity was divided into five categories. Caucasians comprised 41% of the sample while Hispanics comprised 24%. African Americans also comprised 24% of the sample while Asian and Native Americans comprised 11% as can be seen in Figure 4.4.

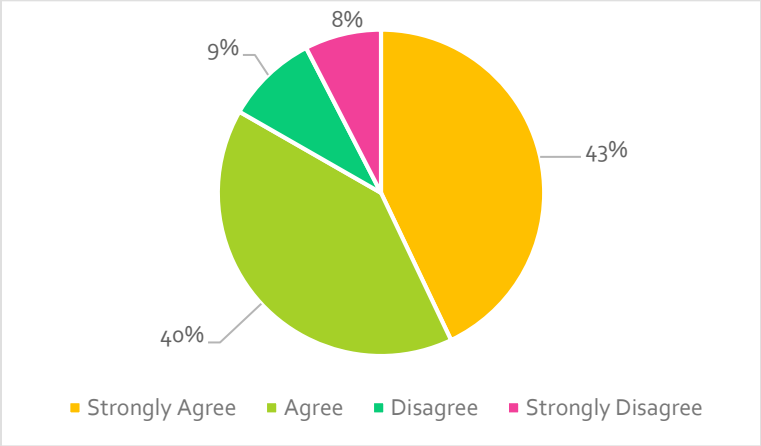
Figure 4.4: Race/Ethnicity of Respondents



[15] Only 7 of the 603 respondents identified themselves as neither man nor women and were removed from the specific questions concerning attitudes analyses because when dealing with percentages, the category of "other" may appear to be more influential than it actually is.

Figure 4.5 shows that the majority of the respondents (83%) felt satisfied with the way they were treated by the police officer (i.e., agreed or strongly agreed with the statement) while 17% were not satisfied (i.e., disagreed or strongly disagreed).

Figure 4.5: Community Members' Satisfaction with Treatment by the Officer[16]



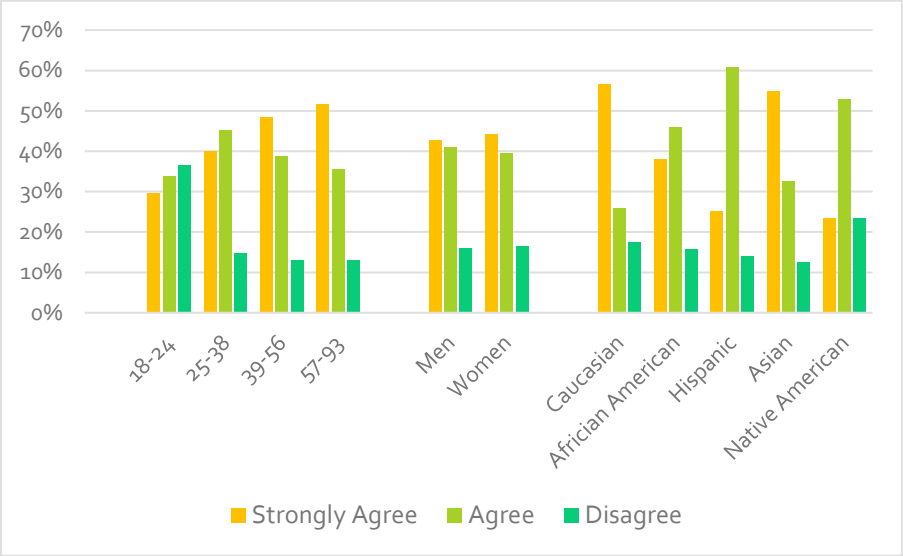
Did the respondents' age affect their perceptions of their treatment by the police officer? Figure 4.6 indicates that it did. Specifically, individuals in the oldest age group are the most likely to say they strongly agree (52%), compared to just 30% of the youngest community members. Conversely, the youngest community members surveyed are more than twice as likely to say they disagree with how they are treated compared to the other age groups. This finding is very similar to other studies' findings concerning age and satisfaction.

Men and women do not appear to differ much with regard to their satisfaction with treatment by the officer. For men, 43% strongly agree with how they are treated, while 41% agree and 16% disagree. Similarly, for women, 44% strongly agree, while 40% agree and 16% disagree.

Our findings also indicate some variation on this question with regard to race/ethnicity. Among Caucasian community members who had a recent interaction with a FCPD officer, 57% said they strongly agree with the statement "I am satisfied with how I was treated by the officer" compared to 26% who agree and 18% who disagree. For African Americans, the percent of those who strongly agree drops to 38% while 46% agree and 16% disagree. Among Hispanics, a quarter of those surveyed strongly agree, while 61% and 14% said they agree or disagree. For Asians, 55% strongly agree, 33% agree and 13% disagree. Finally, among Native Americans, nearly a quarter (24%) strongly agree, while 53% agree and 24% disagree. In sum, our findings indicate that both Caucasians and Asians are the most likely to strongly agree that the officer treated them well, while Native Americans are the most likely to disagree.

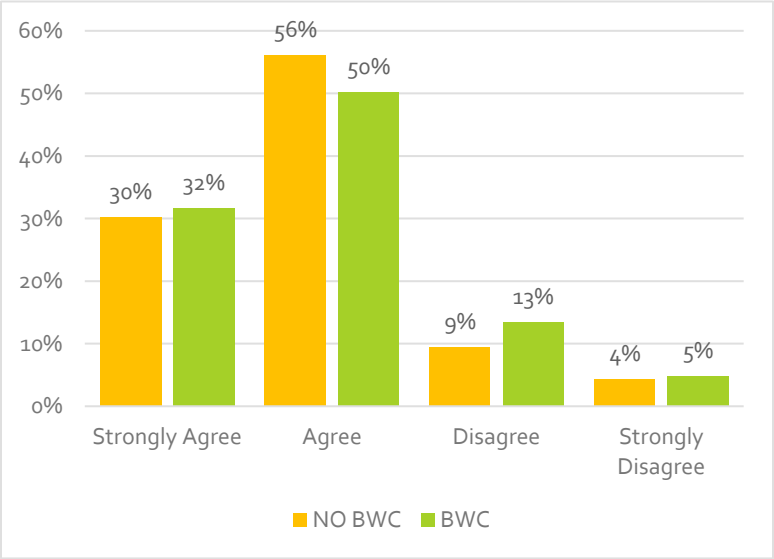
[16] The total might not equal 100% due to rounding error. This is true for all figures in this section.

Figure 4.6: Satisfaction with How I Was Treated by the Officer, by Age, Gender and Race/Ethnicity



Next, we examined whether the presence of a BWC impacted the individual's sense of how well FCPD does its job. As shown in Figure 4.7, 82% of community members who interacted with a BWC officer agree or strongly agree with the statement "The FCPD does its job well" while 18% disagree or strongly disagree. Among those community members who interacted with a non-BWC officer, 86% agree or strongly agree while 13% disagree or strongly disagree. Thus, with respect to perceptions of overall job performance, the response from community members is fairly stable regardless of whether the officer on scene wore a BWC or not.

Figure 4.7: Community Members' Satisfaction with Treatment, by Officer's BWC Status



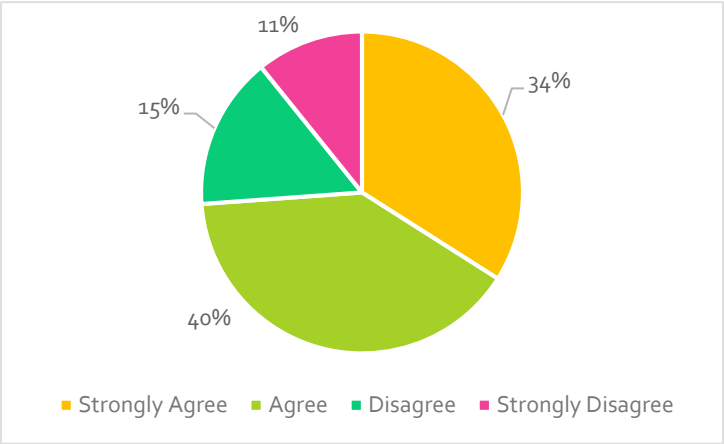
Significance tests (see Figure 4.8 below) confirmed that the two groups did not differ significantly from one another on this question.

Figure 4.8: Student's t-Test Showing Comparisons between Treatment and Control Groups on Satisfaction with Treatment

BWC Status	N	Mean	SD	SEM	t	Results
NO BWC	316	1.804	0.862	0.048	0.759	Not Sig.
BWC	260	1.827	0.928	0.058		

Community members were also asked whether or not they were satisfied with how their situation was resolved. As Figure 4.9 illustrates, the majority of those surveyed agree (40%) or strongly agree (34%) with this statement. This contrasts with a smaller number of respondents who disagreed (15%) or strongly disagreed (11%).

Figure 4.9: Community Members' Satisfaction with How Their Situation Was Resolved



Taking a closer look at this question, Figure 4.10 illustrates the breakdown in satisfaction in how the situation was resolved by age, gender and race/ethnicity. Similar to our findings above for officer treatment, age has a noticeable effect, with the oldest age group (57-93) being most likely to say they strongly agree (52%) compared to just 30% of the youngest age group (18-24). By the same token, the youngest age group is also more than twice as likely to disagree with this statement (37%) compared to the other three age groups.

Men and women are similar in their perceptions of satisfaction with how their situation was resolved. Among men, 43% strongly agree, while 41% agree and 16% disagree. For women, 44% strongly agree, while 40% agree and 16% disagree.

For race/ethnicity, the effects are similar to those presented above, with 57% of Caucasian community members strongly agreeing with the statement "I am satisfied with how my situation was resolved" compared to 26% who agree and 18% who disagree. For African Americans, the percent of those who strongly agree drops to 38% while 46% agree and 16% disagree. Among Hispanics, a quarter of those surveyed strongly agree, while 61% and 14% said they agree or disagree respectively. For Asians, 55%

strongly agree, 33% agree and 13% disagree. Finally, among Native Americans, 24% strongly agree, while 53% agree and 24% disagree.

Figure 4.10: Community Members' Satisfaction with How Their Situation Was Resolved, by Age, Gender and Race/Ethnicity

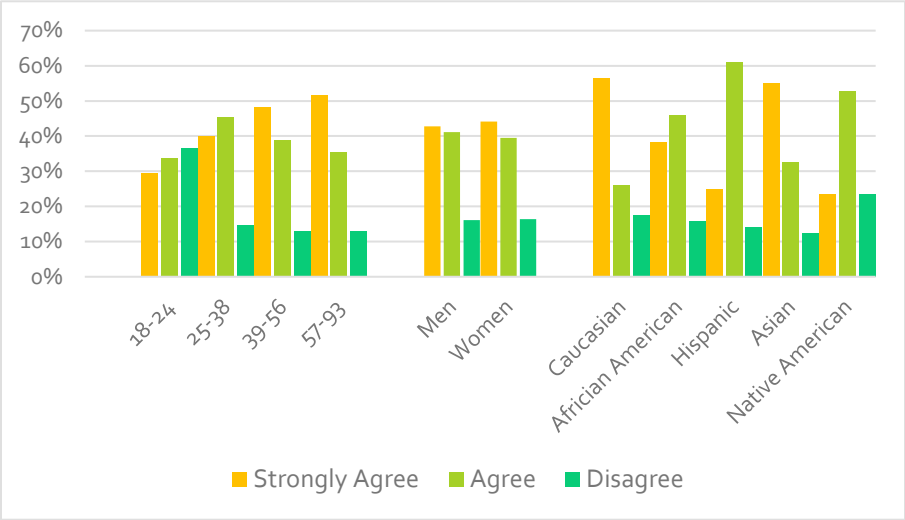


Figure 4.11 shows the breakdown for satisfaction with how the situation was resolved by the BWC status of the officer on scene. Among community members who interacted with a BWC officer, 36% agree and 34% strongly agree with the statement "I am satisfied with how my situation was resolved" while 16% said they disagree and 13% strongly disagree. In comparison, among those who interacted with a non-BWC officer, 34% agree and 42% strongly agree while 15% said they disagree and 9% strongly disagree. Although it appears that community members who interacted with a BWC officer are slightly less likely to report that they are satisfied compared to those who interacted with a non-BWC officer, the significance test (see Figure 4.12 below) confirms that the difference between the two groups is not statistically significant.

Figure 4.11: Community Members' Satisfaction with How Their Situation Was Resolved, by Officer's BWC Status

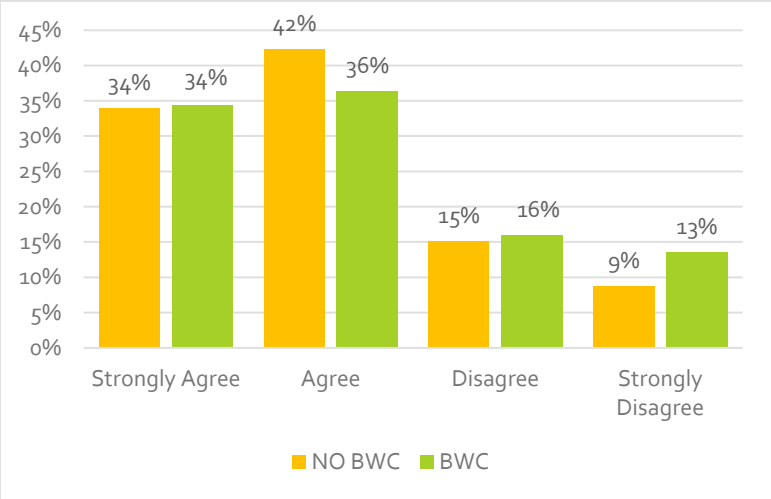


Figure 4.12: Student's t-Test Showing Comparisons between Treatment and Control Groups on Satisfaction with How Their Situation Was Resolved

BWC Status	N	Mean	SD	SEM	t	Results
NO BWC	332	1.994	0.871	0.048	-1.094	Not Sig.
BWC	267	2.077	0.974	0.060		

Respondents were also asked a series of questions regarding their feelings towards FCPD. As shown below in Figure 4.13, when asked if they thought that FCPD does its job well, a strong majority said that they either agreed (53%) or strongly agreed (31%) with this statement compared to only 11% who disagreed and 5% that strongly disagreed.

Figure 4.13: The Department Does Its Job Well

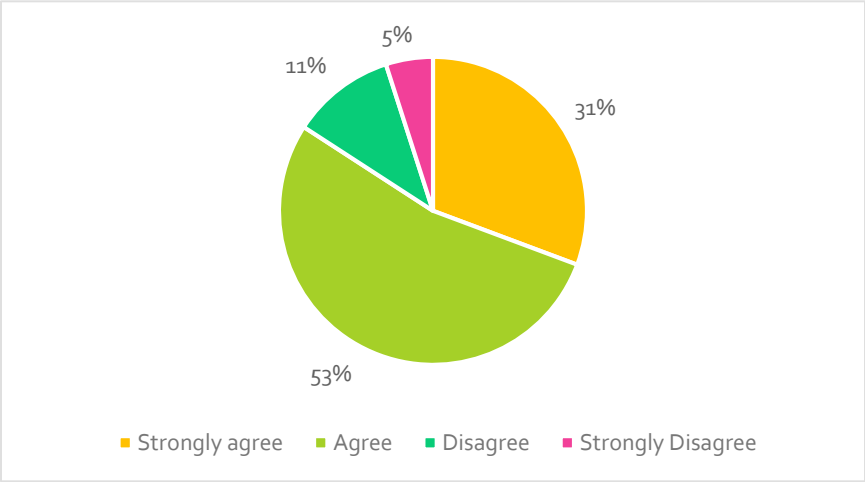


Figure 4.14 illustrates the breakdown in whether community members feel that the FCPD does its job well by age, gender and race/ethnicity. Once again, we find that age has an impact on community perceptions, with the oldest age group (57-93) being most likely to say they strongly agree (44%) compared to just 16% of those aged 18-24. Conversely, the youngest age group is nearly two, to three times more likely to disagree with this statement (32%) compared to the other three age groups.

Our results do not find any major differences by gender regarding the statement that FCPD does its job well. For men, 31% strongly agreed with this statement, while 55% agreed and 14% disagreed. For women, 31% strongly agreed, while 53% agreed and 16% disagreed.

Among Hispanics, 24% strongly agree, while 59% and 18% said they agree or disagree. For Asians, 41% strongly agree, 46% agree and 13% disagree. Finally, among Native Americans, 38% strongly agree, while 44% agree and 19% disagree.

Figure 4.14: Community Members' Belief the FCPD Does Its Job Well, by Age, Gender and Race/Ethnicity

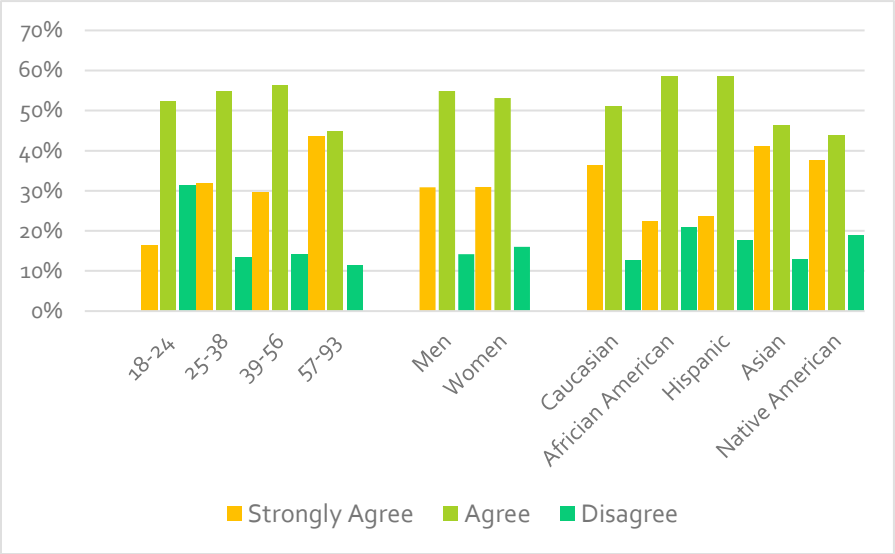
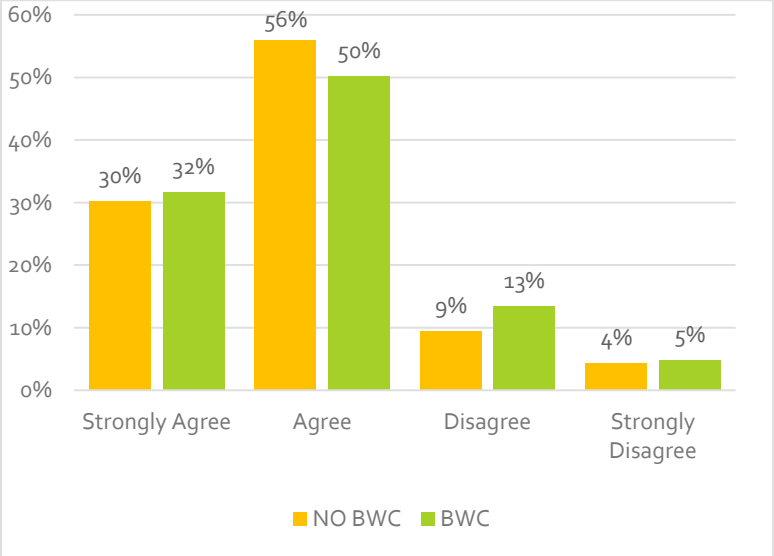


Figure 4.15 presents results on how well FCPD does its job by the BWC status of the officer on scene. Among those who interacted BWC officer, 50% agree and 32% strongly agree with the statement "I am satisfied with how my situation was resolved" while 13% said they disagree and 5% strongly disagree. In comparison, among those who interacted with a non-BWC officer, 56% agree and 30% strongly agree, while 9% said they disagree and 4% strongly disagree.

Figure 4.15: Community Members' Belief that the FCPD Does Its Job Well, by Officer's BWC Status



Although findings for both groups are similar, it appears that community members who interacted with a BWC-wearing officer are slightly less likely to report that they agree that FCPD does its job well compared to those who interacted with a non-BWC officer. Yet the significance test (see Figure 4.16 below) confirms that the difference between the two groups is not statistically significant.

Figure 4.16: Student's t-Test Showing Comparisons between Treatment and Control Groups on Belief that FCPD Does its Job Well

BWC Status	N	Mean	SD	SDM	t	Results
NO BWC	298	1.88	0.747	0.043	0.615	Not Sig.
BWC	231	1.91	0.797	0.052		

The next question asked respondents whether FCPD shares the values of their community. As seen in Figure 4.17, a strong majority of those surveyed either agreed (54%) or strongly agreed (27%) with this statement, while 14% disagreed and only 4% strongly disagreed.

Figure 4.17: The Department Shares the Values of My Community

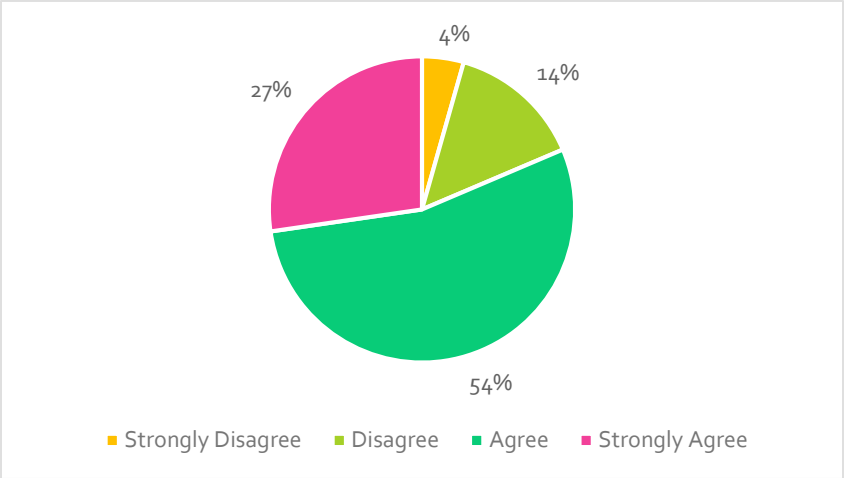


Figure 4.18 illustrates the statistical breakdown in whether community members feel the FCPD shares the values of their community by age, gender and race/ethnicity. A majority of respondents across all age groups agree or strongly agree with this statement. Again, age shows a noticeable impact on community members' perceptions, with the oldest age group (57-93) being most likely to say they strongly agree (42%) compared to just 11% of those aged 18-24. Conversely, the youngest age group is nearly three times more likely to have disagreed with this statement (28%) compared to older community members (11%).

In terms of gender, there are no major differences in whether or not community members feel that FCPD shares the values of their community. For men, 27% strongly agree with this statement, while 54% agree and 17% disagree. Similarly, for women, 27% strongly agree while 55% agree and 18% disagree.

There are strong majorities across all race/ethnicity groups that feel FCPD shares the values of their community. Among Caucasians, 32% strongly agree with this statement, while 54% agree and 14% disagree. For African Americans, the percent of those who strongly agree drops to 20% while 52% agree and 28% disagree. Among Hispanics, 19% strongly agree, while 62% and 20% said they agree and disagree respectively. For Asians, 39% strongly agree, 49% agree and 13% disagree. Finally, among Native Americans, 31% strongly agree, while 63% agree and 6% disagree. These findings indicate broad agreement that FCPD shares the values of their community. At the same time, in comparison to all groups, we also find that African American and Hispanic community members are more likely to disagree with this statement.

Figure 4.18: Community Members' Belief the FCPD Shares the Values of My Community, by Age, Gender and Race/Ethnicity

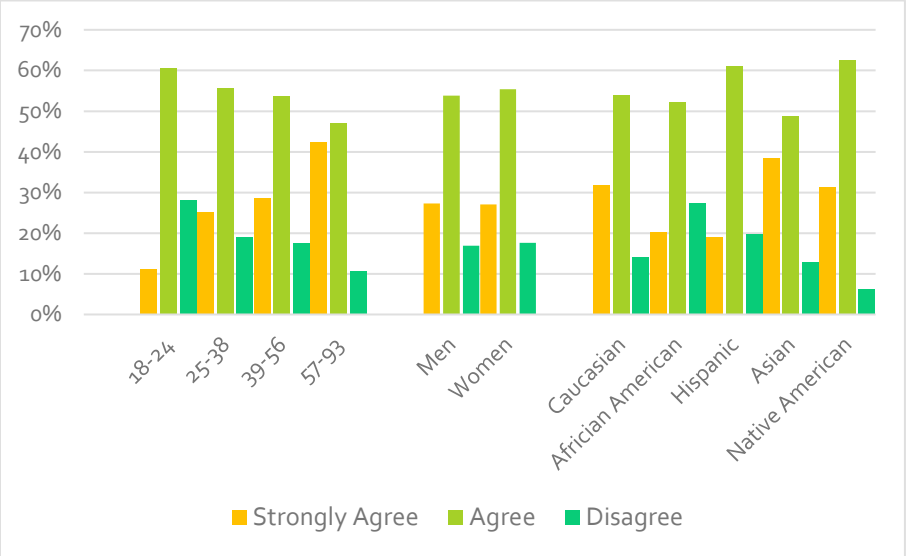
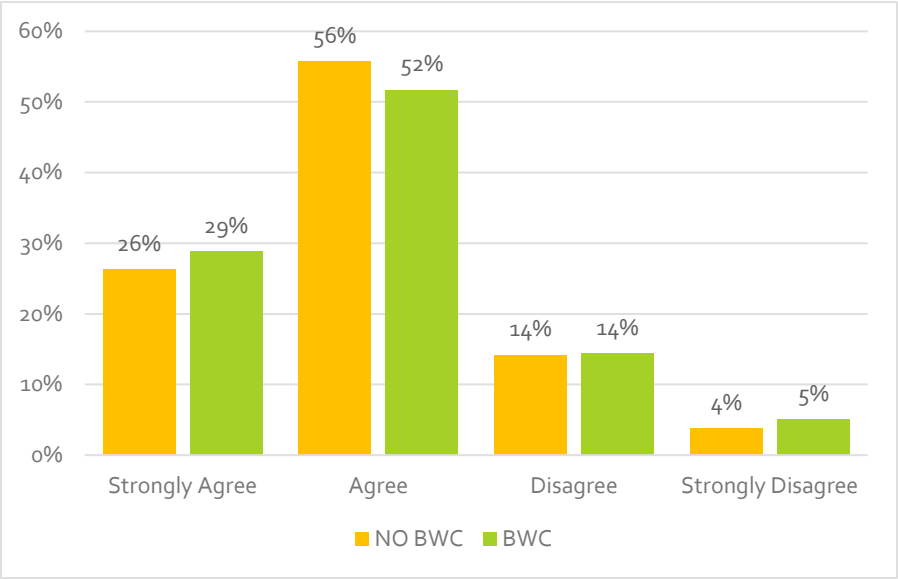


Figure 4.19 displays the results for the question of whether FCPD shares the value of my community by the BWC status of the officer on scene. Again, the differences between groups appear to be minimal. Among community members who interacted with a BWC officer, 29% agree and 52% strongly agree with the statement while 14% said they disagree and 5% strongly disagree. In comparison, among those who interacted with a non-BWC officer, 26% agree and 56% strongly agree while 14% disagree and 4% strongly disagree.

Figure 4.19: Community Members' Belief that the FCPD Shares My Community's Values, by BWC Status



Tests for statistical significance (see Figure 4.20) corroborate the findings presented above, showing a lack of statistical significance. Taken together, the results indicate that the presence of a BWC has no meaningful impact on whether or not community members feel that FCPD shares the values of their community.

Figure 4.20: Student's t-Test Showing Comparisons between Treatment and Control Groups on Belief that the FCPD Shares My Community's Values

BWC Status	N	Mean	SD	SEM	t	Results
NO BWC	289	1.96	0.746	0.044	0.969	Not Sig.
BWC	236	1.96	0.798	0.052		

Next, we examined whether respondents feel they were treated in a procedurally just manner by the officer on scene. [17] As Figure 4.21 illustrates, a majority of respondents (52%) report that they are treated with high levels of procedural justice by the officer while 40% of respondents said they are treated with medium levels of procedural justice. These figures contrast with just 8% who report low levels of procedural justice.

[17] Procedural justice is a concept referring to being treated respectfully, fairly, professionally and that the officer listened to your side of the story and informed you of the decision that he/she was making.

Figure 4.21: Being Treated in a Procedurally Just Manner by Police

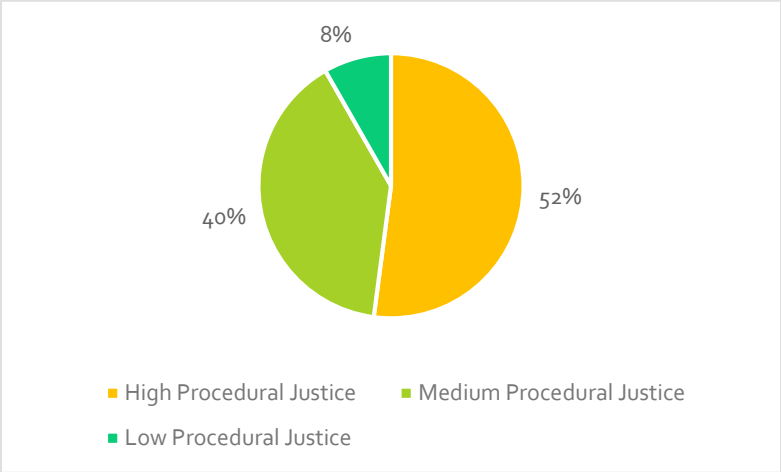
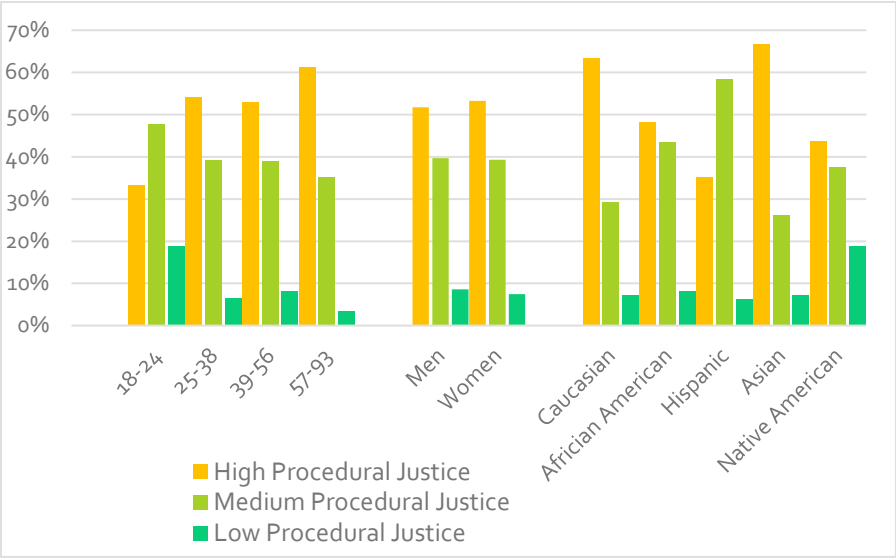


Figure 4.22 illustrates a more detailed statistical breakdown of whether community members feel they were treated in a procedurally just manner by age, gender and race/ethnicity. The majority of all age groups feel that they are treated with either high or medium levels of procedural justice. The findings also indicate that age has an impact on community perceptions, with the oldest age group (57-93) being most likely to say they are treated with high levels of procedural justice (61%) compared to just 33% of those aged 18-24. Conversely, the youngest age group was six times more likely to report experiencing low levels of procedural justice (19%) compared to older community members (3%). Thus, although the majority of all age groups believe that they are treated in a procedurally just manner, younger community members stand apart as being much less likely to share this belief.

The results do not find any major differences between men and women regarding perceived levels of procedural justice. Fifty-two percent of men report high levels of procedural justice, while 40% report medium levels and 9% low levels. For women, 53% report high levels, 39% medium levels and 7% low levels.

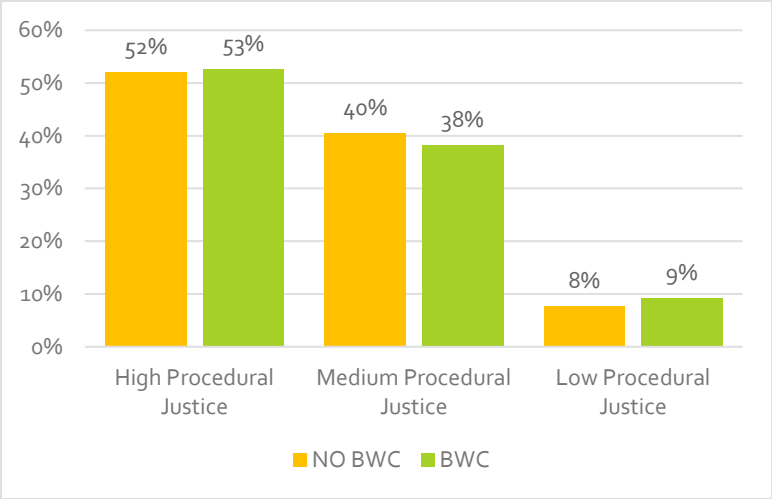
Regarding race/ethnicity, strong majorities across all race/ethnicity groups feel that FCPD treated them with either strong or medium levels of procedural justice although there are substantial differences across the racial groups. Among Caucasians, 63% report high levels of procedural justice, while 30% report medium levels and only 7% report low levels. For African Americans, the percent of those reporting high levels drops to 48%, while 43% report medium levels and 8% low levels. Among Hispanics, just 35% report high levels, 58% medium and 6% low levels. Asians are closer to Caucasians in their perceptions with 67% reporting high levels, 26% medium levels and 7% low levels. Finally, among Native Americans, 44% report high levels of procedural justice, 38% medium levels and 19% low levels.

Figure 4.22: Community Members' Perceived Procedurally Just Treatment, by Age, Gender and Race/Ethnicity



The next analysis investigated whether community members' perceptions of procedurally just treatment varies by the presence of an officer wearing a BWC. As shown in Figure 4.23, perceptions of procedural justice do not vary much by BWC status. Among those who interacted with a BWC officer, 53% report high levels of procedural justice, 38% medium levels and only 9% low levels. Similarly, for those who interacted with a non-BWC officer, 52% report high levels of procedural justice, 40% medium levels and 8% low levels.

Figure 4.23: Community Members' Perceived Procedurally Just Treatment by BWC Status



The tests for statistical significance (see Figure 4.24) corroborated the visual conclusion of no statistical significance. Taken together, the results indicate that the presence of a BWC had no meaningful impact on whether community members felt that the officer treated them in a procedurally just manner or not.

Figure 4.24: Student's t-Test Showing Comparisons Between Treatment and Control Groups on Perceptions of Procedurally Just Treatment by Officer

BWC Status	N	Mean	SD	SEM	t	Results
NO BWC	302	1.7232	0.71244	0.04100	0.391	Not Sig.
BWC	251	1.7761	0.72998	0.04608		

Another survey question asked respondents whether they think BWCs should be worn by all officers. As shown in Figure 4.25, the vast majority of respondents (92%) agreed or strongly agreed with the statement that BWCs should be worn by all officers, not just the community members who interacted with a BWC-wearing officer. Only 8% of those surveyed either disagreed or strongly disagreed, indicating broad support for this technology.

Figure 4.25: BWCs Should Be Worn by All Officers

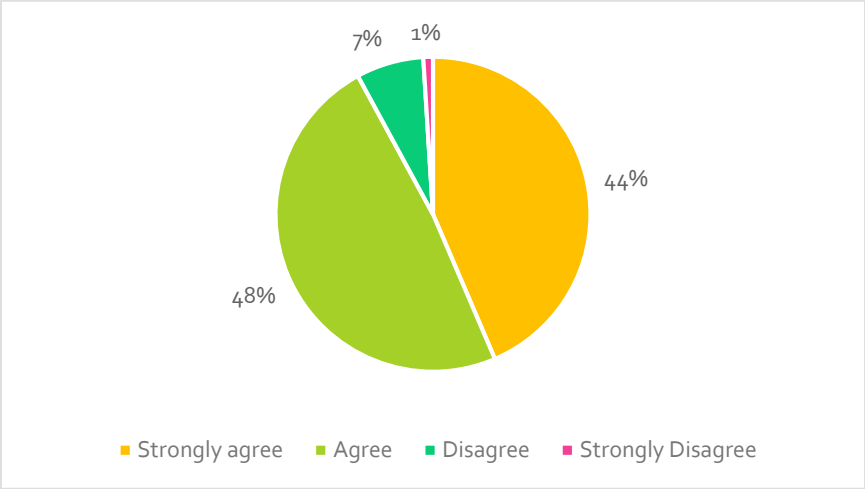
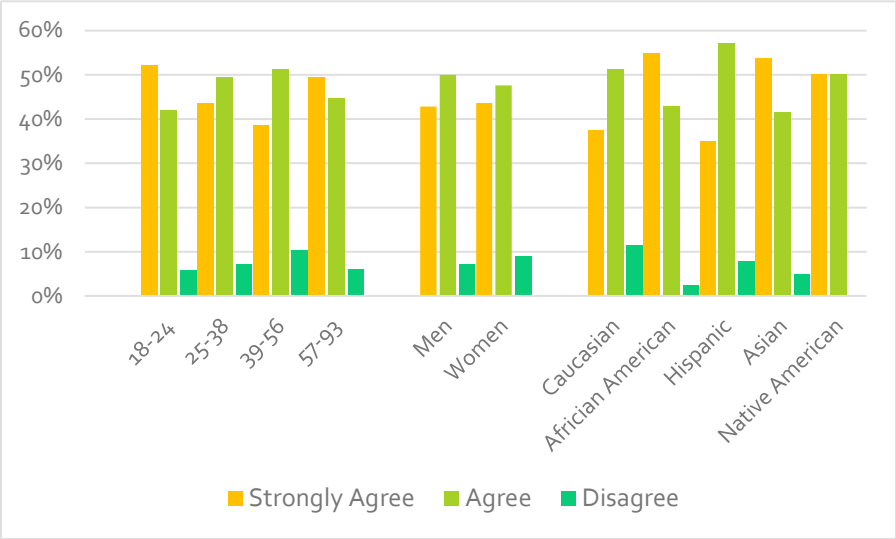


Figure 4.26 displays support for BWCs across age, gender and race. As expected, a majority of community members across all age groups either agree or strongly agree with the statement "BWCs should be worn by all officers." The 18 to 24 age group voiced the most support for this statement, with 52% strongly agreeing and only 6% disagreeing. Conversely, the 39 to 56 age group voices the lowest support for this statement with 39% who strongly agree and 10% that disagree. Men and women are largely in agreement on the question, with large majorities in favor of the idea. Among men, 43% strongly agree, 50% agree and only 7% disagree. For women, 44% strongly agree, 48% agree and 9% disagree.

Our findings also indicate that strong majorities across all race/ethnicity are in favor of BWCs being worn by all officers. Among Caucasians, 37% strongly agree with this statement, while 51% agree and 12% disagree. For African Americans, the percent of those who strongly agree rose to 55% while 43% agree and 2% disagree. Among Hispanics, just 35% strongly agree, while 57% and 8% said they agree and disagree respectively. For Asians, 54% strongly agree, 42% agree and 5% disagree. Finally, among Native

Americans, 50% strongly agree, while 50% agree. These findings indicate broad support for the use of BWCs, although Caucasians are most likely to disagree with the idea.

Figure 4.26: Community Members' Belief that BWCs Should Be Worn by All Officers, by Age, Gender and Race/Ethnicity



Next we examined whether support for the idea that BWCs should be worn by all officers is influenced by whether the officer in the interaction wore a BWC or not (see Figure 4.27). Once again, the differences between the treatment and control groups appear to be minimal. Among community members who interacted with a BWC officer, 48% agree and 45% strongly agree, while 7% said they disagree and only 1% strongly disagree. In comparison, among those who interacted with a non-BWC officer, 49% agree and 43% strongly agree while 7% said they disagree and 1% strongly disagree. Thus, it does not appear that the presence of a BWC has any meaningful impact on whether community members support the use of BWCs for all officers. The test for statistical significance (see Figure 4.28, next page) supports this conclusion.

Figure 4.27: Community Members' Belief that BWCs Should Be Worn by All FCPD Officers, by BWC Status

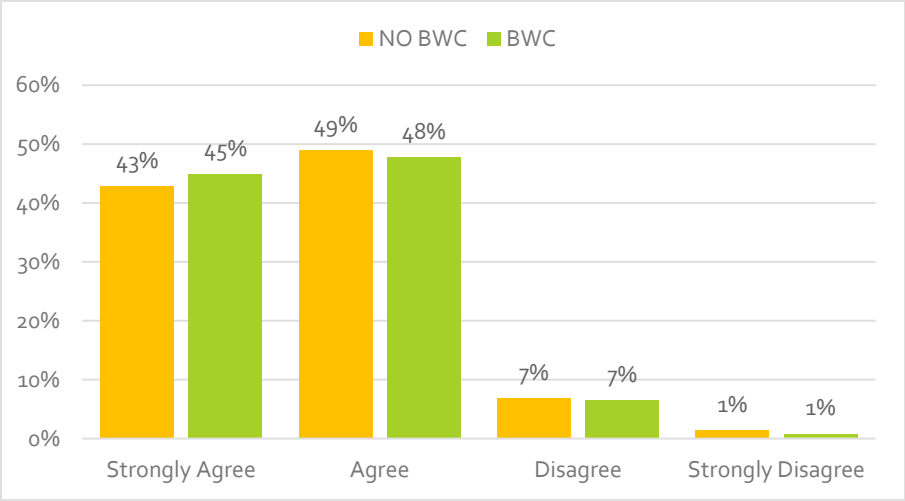
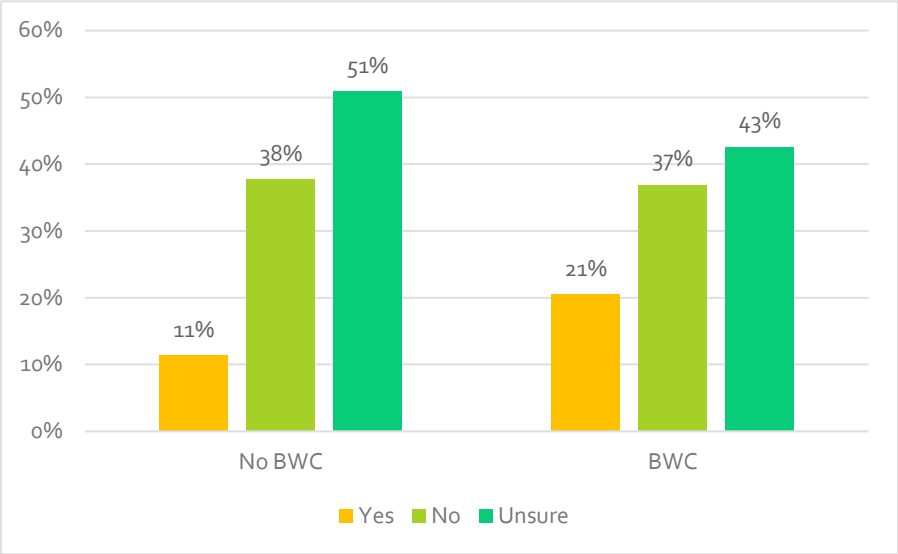


Figure 4.28: Student's t-Test Showing Comparisons between Treatment and Control Groups on BWCs Should Be Worn by All Officers

BWC Status	N	Mean	SD	SEM	t	Results
NO BWC	294	1.67	0.664	0.039	0.561	Not Sig.
BWC	243	1.63	0.644	0.041		

The last question asked respondents if the officer they interacted with wore a BWC. Among those who interacted with a non-BWC officer, the majority (51%) are unsure whether the officer had one while 38% said (correctly) that there was no camera (see Figure 4.29). Interestingly, 11% said a camera was present, even though the officer was not wearing one. Among those who interacted with a BWC-wearing officer, nearly (43%) are unsure about the officer's BWC status, while over a third (37%) incorrectly identified the officer as not wearing one. Only 21% of the treatment group was correctly aware that the officer they interacted with had a BWC.

Figure 4.29: The Community Member's Awareness of BWC during the Encounter



PART C. CONCLUSIONS

First, a majority of respondents express satisfaction regarding their personal interaction with an officer. For example, strong majorities report being satisfied with how the officer treats them and with how the encounter with the police was resolved. Nearly all of those surveyed believe that the officer treated them in a procedurally just manner. These findings indicate that on a personal level, the majority of those who interacted with an FCPD officer during the pilot period recall the interaction in a positive light.

Second, a majority of respondents also view FCPD is a positive light. Strong majorities believe that FCPD does its job well and that FCPD shares the values of the respondent's community. In other words,

among community members who had a recent interaction with the police, most of them report feeling positive not only about their personal experience but also about the department as a whole.

Third, there is overwhelming support among these community members for the widespread adoption of BWCs. Interestingly, there is no evidence that the presence or absence of a BWC during their police encounter has a meaningful impact on their satisfaction with it or the FCPD as a whole.

Fourth, both the age and race/ethnicity of the community member appear to influence their perceptions. Although majorities of all age and racial groups report mostly positive feelings regarding both their personal interactions with an officer and toward FCPD, there are noticeable differences. Older community members are more likely to recall their interaction and the FCPD in a positive light than do their younger counterparts. The same is true for race/ethnicity, with Caucasian and Asian community members expressing more positive feelings about their interactions and FCPD than do African Americans, Hispanic and Native Americans. Not surprisingly, this finding is somewhat reversed when the question turns to whether BWCs should be worn by all officers. The largest percentages of "strongly agree" responses are among young adults (ages 18 to 24) and three minority groups (African Americans, Asians, and Native Americans), but when the percentages of strongly agree and agree are combined, no groups stood apart from the others.

SECTION FIVE:
PERSPECTIVES OF COMMUNITY STAKEHOLDERS

Section Five: Perspectives of Community Stakeholders

SUMMARY OF FINDINGS

- Overall, the community stakeholders' beliefs in the effectiveness of BWCs are cautious and vary by the question asked:
  - Nearly half (41%) agree that BWCs will reduce the number of complaints against police officers.
  - A majority (58%) agree that BWCs will make the police more accountable.
  - Nearly half (47%) agree that BWCs will make the police more legitimate in the community's eyes.
  - A smaller minority (29%) believes that BWCs will reduce the use of force by police.
- Overall, the NGO sub-group of stakeholders (heads of non-governmental organizations) agree at much higher rates than do the governmental sub-group of stakeholders that BWCs are effective in achieving the four outcomes listed above.
- Overall, the vast majority of stakeholders agree that the FCPD involved them adequately in the development of BWC policy (76%), shares the values of their community (76%) and does its job well (88%).

PART A. METHODOLOGY

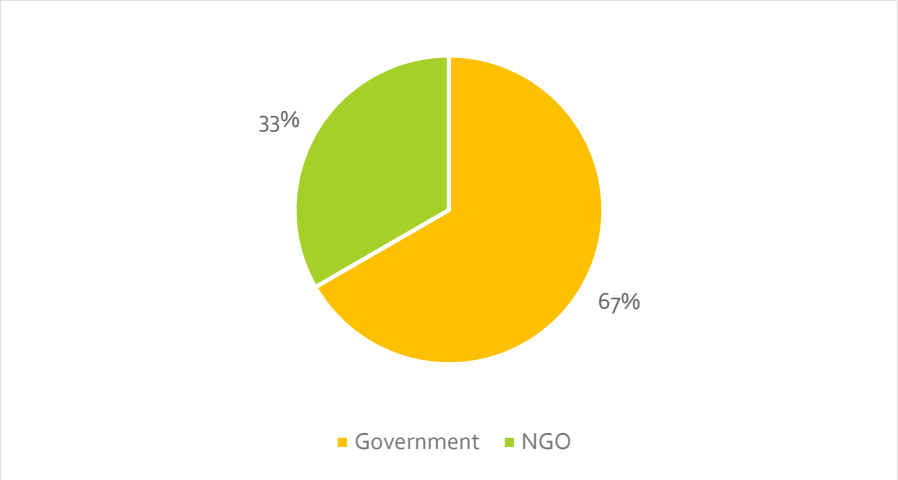
The FCPD recognized early in its decision to conduct the BWC pilot program that input from the community on the policy guiding officer behavior during the pilot would be essential. To that end, it assembled a group of community stakeholders to develop BWC policies while also addressing personal privacy rights and the constitutional safeguarding of individuals in the community. The stakeholders are leaders of special interest, civic and business organizations and as such provide a distinct yet complementary perspective regarding the probable effects of BWCS in their communities. The evaluation research team received permission from FCPD to survey the stakeholders during the pilot period in order to understand their attitudes and expectations regarding the use of BWCs, the potential effects on policing in their communities and the FCPD as a police agency.

The 23 stakeholders were emailed the link to an online survey in June, approximately halfway through the pilot period. Eighteen stakeholders responded to the survey for a 78% response rate. For analysis purposes, the stakeholders are divided into two groups by whether they worked for Fairfax County (government-related) or they represented a non-governmental organization (NGO) in order to see whether differences by type of group exist. This report section presents the results on four questions about the expected effectiveness of BWCs and three questions about the FCPD.

PART B. ANALYSIS OF THE SURVEY DATA

Figure 5.1 shows the percentage breakdown by the stakeholders' affiliation. Two-thirds (67%) were affiliated with the Fairfax County government while the remaining 33% were leaders of special interest, civic or business organizations.

Figure 5.1: Stakeholders' Affiliation



Perceptions Concerning the Likely Effectiveness of BWCs

Seventeen Likert-like items were asked of the stakeholders along with several open-ended questions. Likert survey items typically present a statement and ask the respondent to indicate the strength of their agreement or disagreement to it on a 5-point scale with "neither agree nor disagree" as the middle category. Our survey used four-point response scales ranging from strongly agree through agree, disagree, and strongly disagree to make the respondents choose a position. There was also an option for the respondent to indicate "don't know." This section of the report focuses upon four statements the researchers considered most relevant to the deployment of BWCs:

- BWCs will reduce complaints against police officers.
- BWCs will make the police more accountable.
- BWCs will make police more legitimate in the eyes of my community.
- BWCs will lessen the use of force by police.

Figure 5.2 presents the stakeholders' assessment as to whether the use of BWCs will reduce community members' complaints against FCPD officers. Less than half (41%) of the stakeholders agree with that as a likely outcome, with the majority (53%) disagreeing or strongly disagreeing with it and 6% indicating they don't know. Thus, the shareholders believe that BWCs alone are unlikely to reduce the number of complaints against police officers.

Figure 5.2: BWCs Will Reduce Complaints Against Police Officers

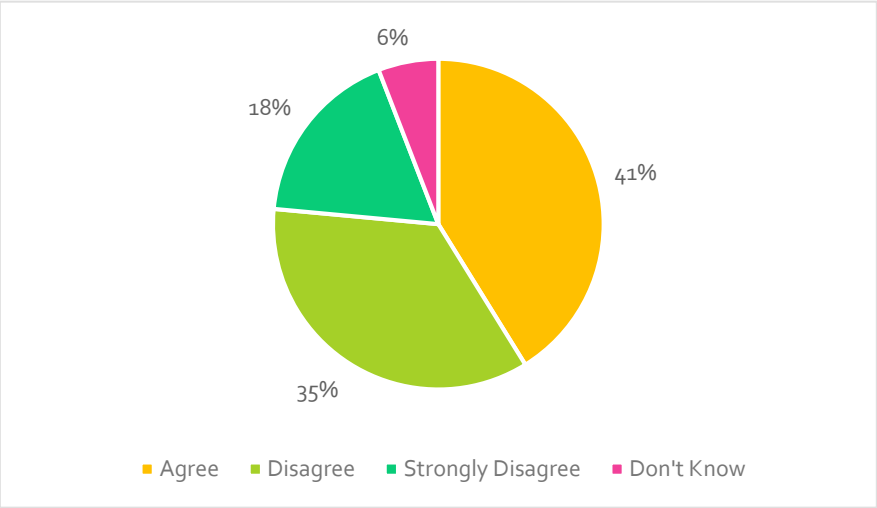


Figure 5.3 presents the preceding statement broken down by the affiliation of the stakeholder. Although all NGO stakeholders agree with the statement, very few (9%) of the government stakeholders agree and the vast majority of them (82%) disagree or strongly disagree. The difference in attitudes between the stakeholder sub-groups is stark.

Figure 5.3: BWCs Will Reduce Complaints Against Police Officers, by Affiliation

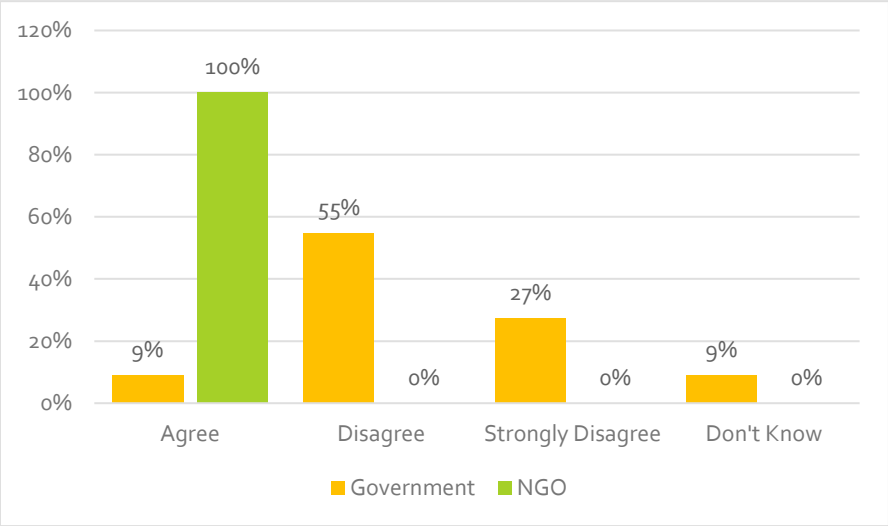


Figure 5.4 shows the percentage distribution for the statement that BWCs will make the police more accountable. Here, the majority (58%) agree or strongly agree, 30% disagree or strongly disagree, and 12% indicated they don't know. The results presented in Figure 5.5 indicate that the NGOs continue to be more positive about the impact of BWCs, with 100% of them agreeing or strongly agreeing that with the accountability statement. As found previously, the government-based stakeholders are less positive, with only 36% agreeing, 45% disagreeing or strongly disagreeing, and the remaining 18% indicating they don't know.

Figure 5.4: BWCs Will Make the Police More Accountable

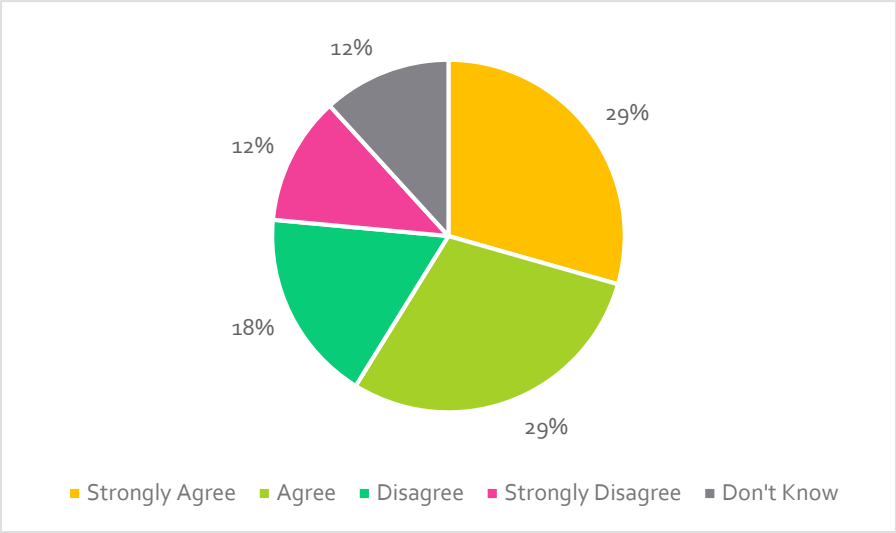


Figure 5.5: BWCs Will Make the Police More Accountable, by Affiliation

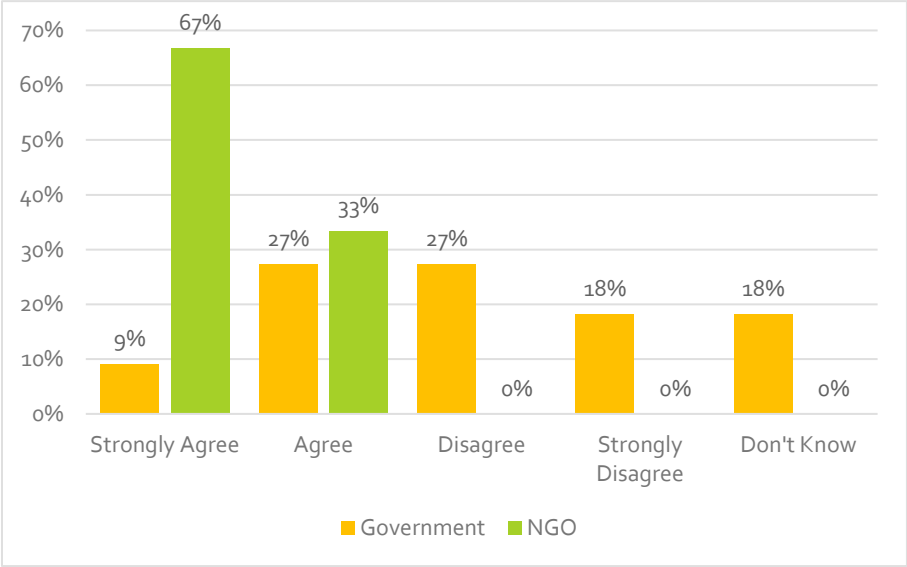
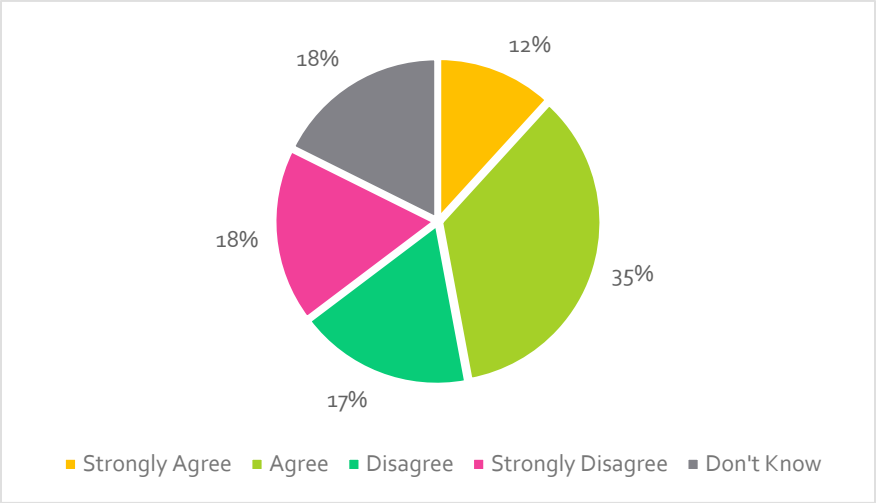


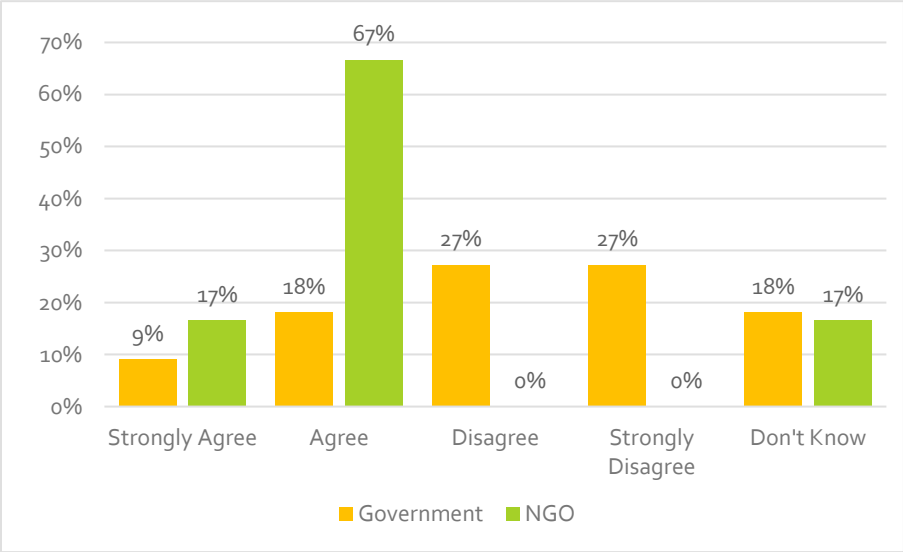
Figure 5.6 presents the findings for a third statement: that BWCs will make the police appear more legitimate in the eyes of one's community members. Nearly half (47%) of the stakeholders agree or strongly agree with the statement while 35% disagree or strongly disagree and 18% don't know.

Figure 5.6: BWCs Make Police More Legitimate in the Eyes of My Community



The breakdown of these responses by stakeholder affiliation, shown in Figure 5.7, marks a small departure from the pattern apparent in earlier results. This time, the NGO stakeholders are nearly in unanimous agreement (84%) but 17% of them indicate they don't know whether the deployment of BWCs would increase perceived police legitimacy. In contrast, only 27% of the governmental stakeholders agree or strongly agree with the statement, the majority (54%) disagree or strongly disagree, and a similar percentage (17%) indicated they don't know.

Figure 5.7: BWCs Will Make Police More Legitimate in the Eyes of My Community, by Affiliation



After the killings of community members in Baltimore, Ferguson, Cincinnati, and North Charleston, one of the most frequently heard reasons for adopting BWCs is the hope that they will reduce the use of force, especially lethal force, by police officers. Figure 5.8 shows that only 29% of the stakeholders agree or strongly agree with that statement and a much larger percentage (42%) disagree or strongly disagree with it. This statement also generated the largest percentage (29%) of don't knows of the four statements.

Figure 5.8: BWCs Will Lessen the Use of Force by Police

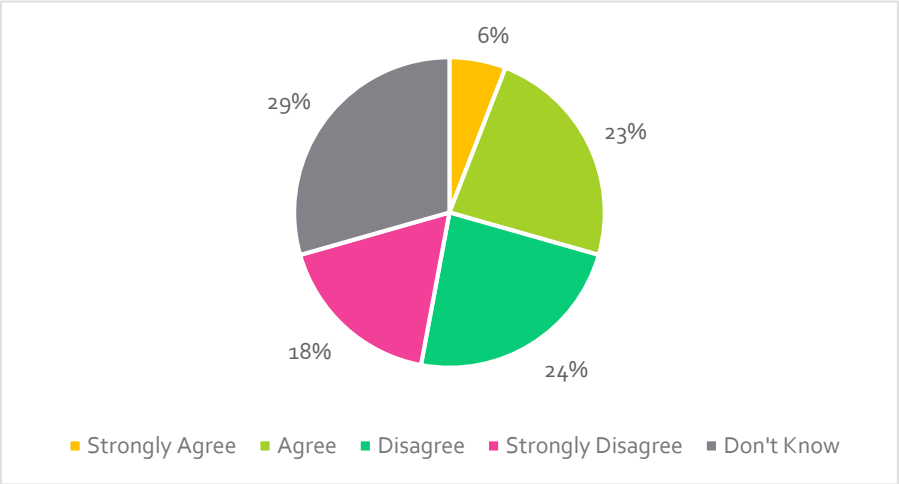
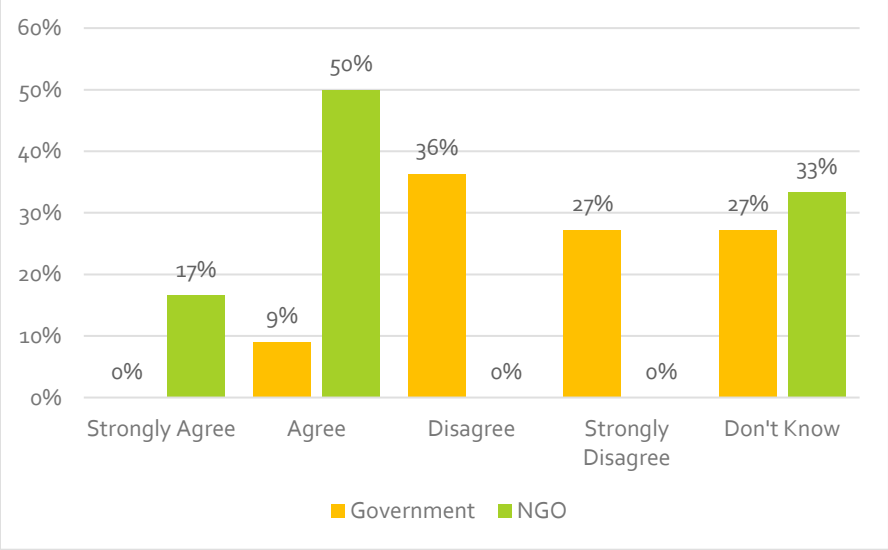


Figure 5.9 shows how the two groups of stakeholders differ on the statement. Again, the NGOs are more positive with 67% of them agreeing or strongly agreeing that the cameras will have a dampening effect on the use of force while a majority of governmental stakeholders (63%) disagree or strongly disagree that they will. "Don't know" was chosen by relatively large percentages of governmental (27%) respondents. This finding confirms a definite trend in responses by stakeholder group: NGOs consistently believe that the effect of BWCs is positive, while the governmental group holds more negative views

Figure 5.9: BWCs Will Lessen the Use of Force by Police, by Affiliation



Attitudes regarding the FCPD

The stakeholders' survey included three other statements rated on the same four-point scale:

- I believe I was adequately involved in the development of the BWC policy.
- The Fairfax Police Department shares the values of my community.
- The Fairfax County Police Department does it job well.

The analyses of responses below follows the same format as the previous section, with a figure and text on the responses of all stakeholders combined and then a figure and text showing responses by the government and NGO sub-groups.

The stakeholders were asked if they were adequately involved in making BWC policy because the articulated role of the stakeholder was to aid the department in drafting policy that ensured that privacy rights and the constitutional protections of community members were adequately addressed. Figure 5.10 shows that the stakeholders agree or strongly agree that they are adequately involved in the process (76%). Only 18% of the group disagree or strongly disagree with the statement.

Figure 5.10: As a Stakeholder, I Was Adequately Involved in Making the BWC Policy

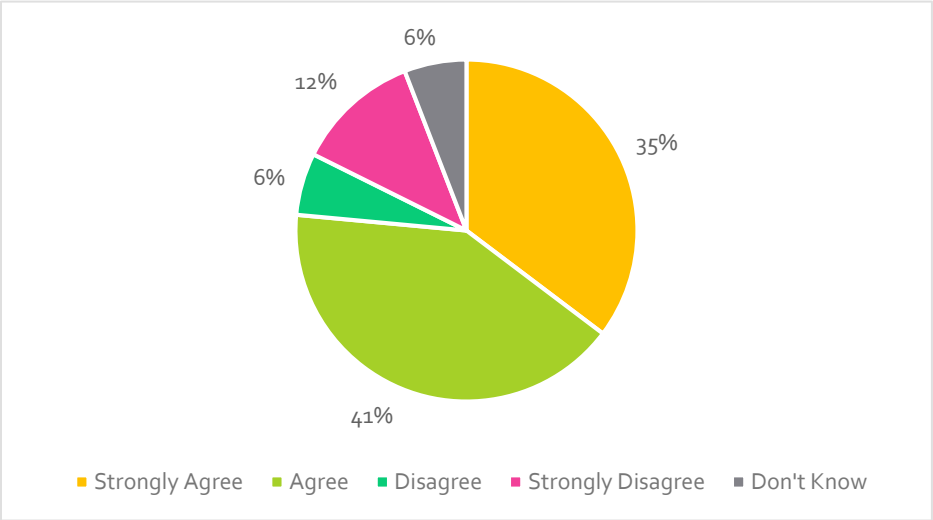
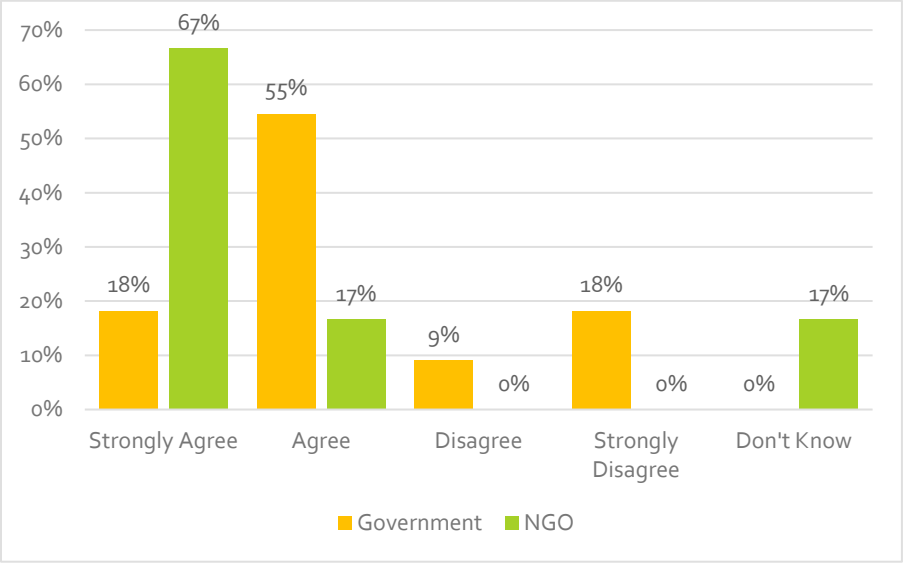


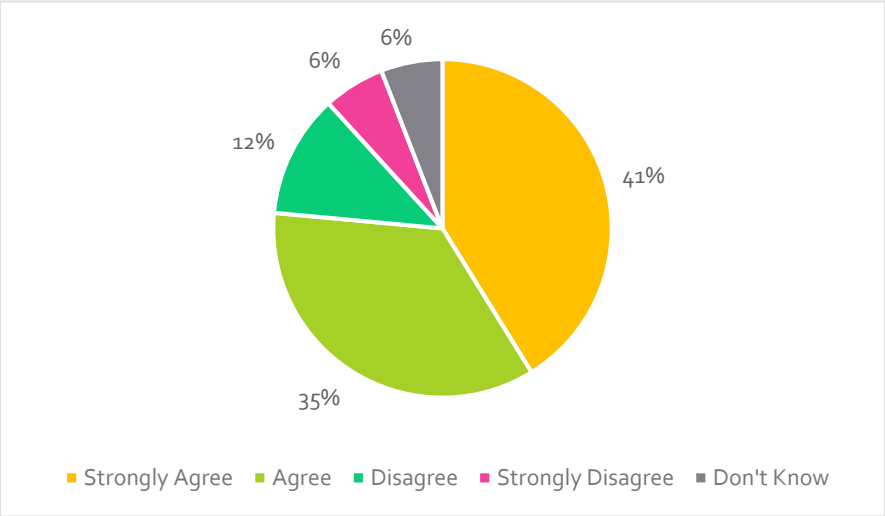
Figure 5.11 evaluates the adequacy of involvement by stakeholder group. As one can see, both groups believe that they were adequately involved. A higher proportion of the NGO sub-group strongly agree (67%) than in the government group (18%), but both groups have a similarly positive viewpoint when the two agree categories are combined (73% and 84% for the governmental and NGO sub-groups, respectively). Several (17%) NGO members responded that they don't know whether they were adequately involved or not.

Figure 5.11: As a Stakeholder, I Was Adequately Involved in Making the BWC Policy, by Affiliation



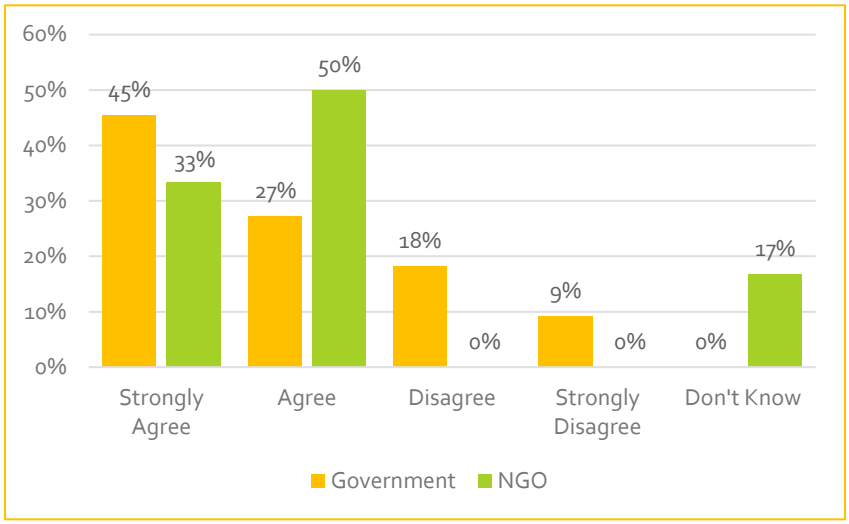
The vast majority of stakeholders (76%) agree or strongly agree that the FCPD shares the values of their community. As seen in Figure 5.12, only 18% disagree with the statement while 6% have no opinion.

Figure 5.12: The FCPD Shares the Values of My Community



Both groups seemed to agree that the FCPD shares their community's values as seen in Figure 5.13. A merging of the strongly agree and agree categories shows that a vast majority of both groups hold similar positive views (72% and 83% for governmental and NGO, respectively). Only 27% of the government stakeholders disagree or strongly disagree while none of the NGOs do.

Figure 5.13: The FCPD Shares the Values of My Community, by Affiliation



Finally, Figure 5.14 shows that the overwhelming majority (88%) of stakeholders believe that the FCPD does its job well. In contrast to many of the earlier analyses, it is the governmental stakeholders that are positive, with 64% strongly agreeing that the FCPD is doing a good job, a level that is almost twice that of the NGO stakeholders (33%). However, when the two agree categories are combined, the governmental stakeholders (91%) and the NGO stakeholders (83%) are almost equally positive regarding FCPD's performance. Only 9% of the governmental stakeholders disagree with the statement while none of the NGO stakeholders do. Only 17% of the NGOs indicated they don't know enough about the FCPD to respond while none of the government stakeholders feel that way. These results suggest that the stakeholders will continue to be a valuable resource for the department as it continues to take the pulse of its community on police matters.

Figure 5.14: The FCPD Does Its Job Well

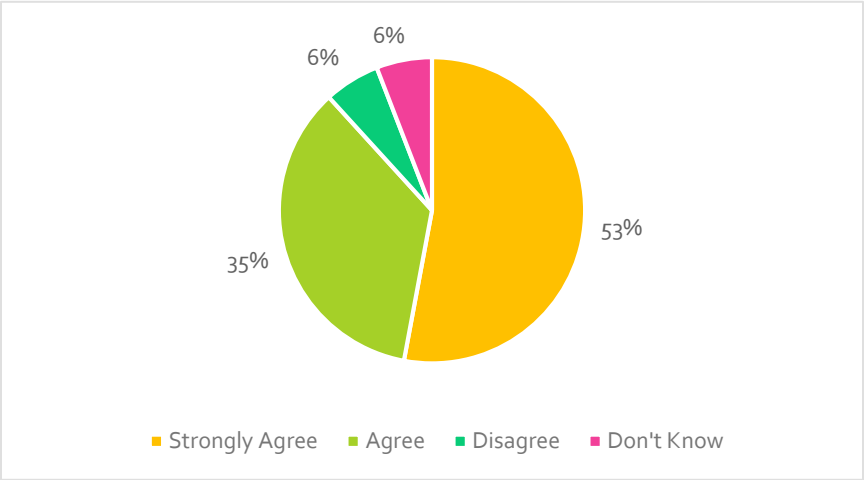
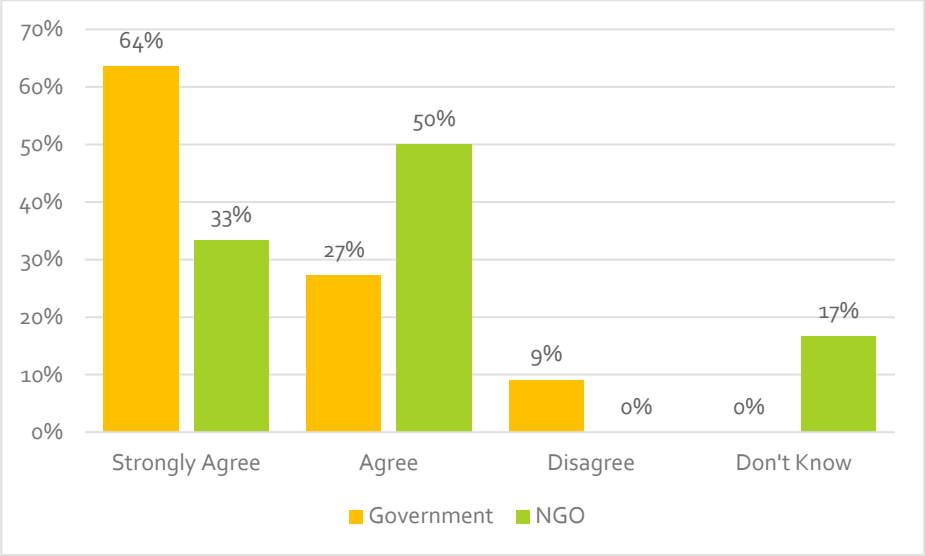


Figure 5.15: The FCPD Does Its Job Well, by Affiliation



PART C. CONCLUSIONS

The community stakeholders provide a valuable perspective on the BWC pilot program in addition to their assistance on BWC policies. Their responses regarding possible effects of BWCs on their communities are cautious: less than half agree that BWCs will reduce complaints against police officers, make the police more legitimate in the eyes of their community members, or lessen the use of force. Only the statement that BWCs will make the police more accountable, agreed or strongly agreed to by 58%, garnered an agreement rate above the 50% level. Clearly and not surprisingly, the use of BWCs alone is not seen by the stakeholders as a way to resolve community-police problems.

The distinction between stakeholders heading up government-related organizations and those leadings NGOs provides valuable insights. The NGO leaders are much more positive about the effects of BWCs than are the government-based leaders. The NGOs unanimously agree that BWCs will reduce complaints against police officers and make the police more accountable. The majority of them also agree that BWCs will make the police more legitimate in the eyes of their community members and would lessen police use of force. None of these four statements were agreed to by more than 36% of the government stakeholders. When presented with statements about the FCPD, however, the vast majority of both groups are positive. More than 71% of the government sub-group agree to each of the three statements and more than 83% of the NGOs do too. It would be interesting to learn why the government stakeholder are underwhelmed by the likely positive effects of BWCs and why the NGOs are so optimistic.

There is an important caveat to these interpretations. It is possible that the community members thought the survey focused on the effects of BWCs only over the six months of the pilot period and only in the three specific pilot stations, rather than the effects of BWCs over a longer period of time and when deployed across all FCPD stations. This is a second question whose answer would be worth knowing.

SECTION SIX:

Synthesis of Evaluation Results and Study Conclusions

Section Six: Synthesis of Evaluation Results and Study Conclusions

The five previous sections of this report have presented detailed information on how the FCPD's pilot BWC program was implemented, what its evaluation included, and what the analyses of data showed. The purpose of this final section is to synthesize the results and offer a clear presentation of the major findings from the quasi-experimental randomized trial study.

Conducting a comprehensive evaluation of a pilot program is challenging. It requires the coordinated development of research instruments and data collection timelines, plus verification that planned program changes actually occurred. The evaluated organization must be responsive to requests for data, personnel and facilities. Above all, the research must be carried out with complete independence. The FCPD cooperated fully with the study design and research team. None of the standard threats to validity and reliability of study results were encountered.

The concentric circles figure from Section One (here labeled Figure 6.1: Context of BWC Decisions and Policies) is a helpful reminder of the multiple sources which have provided perspectives or empirical baselines via this study. Their attitudes, comments and trend lines form the context within which the BWC adoption decision will be made. If BWCs are implemented throughout the department, the same context will exist as the department writes its standard policies and officers then work in conformity with them.

Figure 6.1: Context of BWC Decisions and Policies

The evaluation has shown that the three key audiences expect the impact of BWCs, if implemented, will be minimal. Police officers believe that neither their behavior nor that of community members will change. They anticipate some positive outcomes such as better evidence collection, complaint settlement and greater transparency of the organization to the public but they do not expect BWCs alone to enhance police-community relations. Specifically, they do not expect BWC will improve their legitimacy in the eyes of community members, improve community relations or increase officer safety as they patrol and respond to incidents in their assigned communities.

Officer performance patterns established in the 12 months (9 months for complaints and use of force) preceding the pilot period were unchanged during the 6-month pilot and the 3 months after it. The numbers of traffic stops conducted, incidents responded to, citizen complaints filed and use of force reports evidenced low and level trend lines over the 18-month period examined.

The presence of a BWC made little impact on the community members who were interviewed soon after interacting with an officer. Many did not know whether the officer was wearing a BWC and community members that were aware responded to questions in the same way as their less-aware neighbors. When asked whether FCPD should adopt BWCs department-wide, nearly all agreed. At the same time, the community members expressed strong support for FCPD and its officers. The vast majority believe the department does its job well and shares the values of their community. This was also apparent in the high percentages that indicated their satisfaction with how they were treated by the officer and how the situation was resolved.

The stakeholders hold modest expectations for BWCs. Less than half believe the cameras will reduce the number of complaints against officers, reduce their use of force, or increase their perceived legitimacy. About half expect increased police accountability. Like the community members surveyed, they are very supportive of the FCPD. Over three-quarters agree that the FCPD shares the values of their community and does it job well. The vast majority also feel adequately involved in the development of BWC policy that governed their use during the pilot period.

The overall context is supportive for whatever FCPD decides to do regarding BWCs. The department's key audiences – its police officers, community members and community stakeholders – hold somewhat different but appropriate and achievable expectations should BWCs be deployed agency-wide. If the decision is not to deploy them, the high regard for the department will lead nearly everyone to conclude that it was the right decision for all.

Appendix A: Literature Review

APPENDIX A. LITERATURE REVIEW

The implementation of body-worn cameras (BWCs) has far outpaced evidence-based research on its impacts and effectiveness. As of June 2018, approximately 70 studies had been conducted by academics, the majority of which used U.S. data.[18] One study found that by 2016 about 80% of departments with BWCs cited the main reasons for implementation were to: increase evidence quality, reduce civilian complaints, improve officer safety and reduce agency liability.[19] As a counterpoint, concerns have been raised that increased oversight of officer behaviors and fear of agency liability may result in increased sanctions by supervisors for small technical violations.[20]

Improved quality and availability of evidence is often an expectation of both officers and external stakeholders.[21] This expectation has some solid support in the literature, as implementation of BWCs has resulted in an increase in domestic violence evidence, arrests, charges, prosecution, guilty pleas, and guilty verdicts in two different studies.[22] BWCs may also increase accuracy in officer reports if footage is used to bolster an officer's memory of specific incident details or statements.[23]

The presence of BWCs has also been theorized to have a "civilizing" effect on both citizen and officer behavior during interactions, possibly leading to a reduction in complaints and use of force incidents while increasing overall officer safety. When the risk of being recorded and held accountable for improper behavior increases, deterrence theory would suggest greater community member compliance with officer orders and increased policy compliance by officers.[24] Increased observation by peers, including through camera-recorded methods, has also been linked by social influence and social impact theorists to modified behavior better reflecting societal norms.[25] This would suggest that the use of BWCs will pressure both community members and officers to shift their behavior to more socially and organizationally acceptable actions, thereby reducing violence and other improper actions during interactions. However, research evaluating whether these expectations are borne out in practice have shown mixed results.

Modified officer behaviors that reflect procedural justice treatment of community members such as better listening, voicing decision making options and fair treatment, have consistently shown significant increase in community satisfaction and cooperation with a department.[26] A recent study conducted in one agency found that officers incorporated more procedurally just behaviors following BWC implementation.[27] Another study also found that a citizen's rating of procedural justice during an

---

[18] For a comprehensive review of BWC studies, see Lum et al.'s *Research on body-worn cameras: What we know, what we need to know* (2019).
[19] Hyland, 2018
[20] Jennings et al, 2014; Terril & Reisig, 2003; Maskaly et al., 2017, citing Jennings et al., 2014; Paoline, 2001
[21] Gaub et al., 2018; Goodall, 2007; Jennings et al., 2015; White et al., 2018b
[22] Morrow et al., 2016; Owens et al., 2014
[2323] Lum et al., 2019
[24] Ariel et al., 2017
[25] Ernest-Jones et al., 2011; Ratcliffe et al., 2009; Wahl et al., 2010; Munger and Harris, 1989; Wicklund, 1975
[26] Hinds & Murphy, 2017; Jackson et al., 2012; Mazerolle et al., 2013; Tyler, 2006; Tyler, 2004; Sunshine & Tyler, 2003; Tyler, 1988; Sunshine & Tyler, 2003; Tankebe, 2013; Tyler, 1990; Tyler & Fagan, 2008; Johnson et al., 2014; Mastrofski et al. 1996; Tyler & Huo, 2002; McCluskey, 2003; Reiss, 1971; Wells, 2007
[27] McClusky et al., 2019

encounter was more powerful than the presence of a BWC in predicting satisfaction, even when a BWC was not accurately observed and/or reported.[28]

Regarding citizen behavior, some studies[29] have shown that BWCs may result in increased community member resistance and assaults against police officers. Notably however, there are several studies have indicated no effect or null findings for similar situations.[30] BWCs produced small reductions in overall crime in three studies conducted within the United Kingdom, but more recently, Ariel et al (2016) found no significant effect between crime rate and BWCs.[31] Current limited findings from at least three studies indicate that BWCs may have no effect or reduce citizen willingness to provide investigatory information, resulting in decreased cooperation between civilians and police.[32] Additional studies showed that officer attitudes about the possible civilizing effect of BWCs on community members after BWC implementation became more cynical and less optimistic over time.[33]

Potential reductions in use of force and complaints have been theorized as effects from changed behavior by both officers and civilians. Officers may be less likely to utilize force when unnecessary and/or citizens may be more compliant with officer direction or less likely to complain when video evidence is being gathered. Study results have varied widely on use of force incidents, with impacts ranging anywhere from a 26% to 59% overall reduction in use of force; some studies have even shown no statistically significant differences after the introduction of BWCs.[34] Researchers have documented reductions in citizen complaints after BWC implementation ranging from 12% to 93%, again with a few studies that found no effect at all.[35]

These wide variations in outcomes may be a result of differences in how BWCs are implemented, departmental policies on their use, or lack of buy-in by officers during the introduction of the new technology.[36] One study found that when BWC activation was officer-prompted, officer compliance with activation policy was only 30%.[37] Another study found that officers that followed BWC policy saw a decline of use of force incidents, while those that did not follow policy experienced an increase in use of force incidents.[38]

Demographic characteristics may also affect both officer and community member opinions and behaviors. Findings have largely been mixed on the effect of officer demographics on their behavior, decision making, and citizen complaints, with some indication of differences between officers of different genders, age, and race.[39] Officer perceptions of BWCs vary by individual agency, of course, but

---

28 McClure et al., 2017

29 Ariel et al., 2016a; Ariel et al., 2018; Toronto Police Service, 2016. One study documented an increase in assaults against officers equipped with BWCs but a decrease in the department's overall numbers. (Ariel et al. 2018)

30 Grossmith et al, 2015; Headley et al., 2017; Hedberg et al., 2016; Katz et al, 2014; White et al., 2017

31 Ellis et al., 2015; Goodall, 2007; ODS Consulting, 2011

32 Edmonton Police Service, 2015; Grossmith et al., 2015; Toronto Police Service, 2016

33 Gaub et al., 2016; Headley et al., 2017; White et al., 2018b

34 Reduction: Ariel et al., 2015; Braga et al., 2018b; Jennings et al., 2014; White et al., 2017. No effect: Ariel et al., 2016a; Edmonton Police Service, 2015; Grossmith et al., 2015; Yokum et al., 2017

35 For example, see: Ariel et al., 2015; Ariel et al., 2017; Hedberg et al., 2017; Jennings et al., 2015; Katz et al., 2014, Edmonton Police Service, 2015

36 White et al., 2018b

37 Hedberg et al., 2017

38 Ariel et al, 2016a

39 For example, see Worden, 1989; Brown & Frank, 2007; Smith & Klein, 1983; Sun & Payne, 2004; Brooks, 2001; Engel & Worden, 2003; Sherman, 1978; Alpert, 1989; Fyfe, 1988

studies have consistently found that acceptance increases, or opinions neutralize, over time with BWC experience.[40] Officers that were higher-ranking, more educated, or women have been shown to have higher levels of acceptance for BWCs and other new technology.[41]

While there is general support among the public for BWCs, a national survey found that younger citizens had greater confidence in the ability of BWCs to improve overall relations and trust and to decrease racial tensions. The same survey found that African American respondents were less likely than others to believe in the ability of BWCs to increase transparency, improve relations or increase trust.[42] Both age and education have shown positive linear correlations with satisfaction with police, while minority and lower-class status is tied to less favorable satisfaction levels.[43] Gender influence on satisfaction has shown mixed results.[44]

Overall, the number of studies on BWC implementation, acceptance by both police officers and community members, and consequent changes in outcomes has grown exponentially over the past several years. Many of the studies are descriptive, simply reporting survey results or changes in departmental crime statistics after BWC implementation. Implementation often precedes the recognition that researchers could be helpful, so attitude surveys are based on recall which is well known to not be fully reliable. The reality is that well-designed, rigorously conducted evaluations have been rare. This study by the Fairfax County Police Department, however, is one of them. It promises to inform the department's decisions regarding implementation, other police officials cautiously considering whether to adopt BWCs, and the community of researchers and practitioners eager to disseminate good practices.

[40] Gaub et al., 2016; Ellis et al, 2015: Gaub et al., 2018; Jennings et al., 2014; Jennings et al, 2015; Headley et al., 2017
[41] Kyle & White, 2017; Gramagila & Phillips, 2017; Telep, 2017
[42] Sousa et al., 2017
[43] Reisig & Parks, 2000; Decker, 1981; Apple & O'Brien, 1983; Boggs & Galiher, 1965; Scaglion & Condon, 1980; Smith & Hawkins, 1973; Gallagher et al., 2001; Sampson & Bartusch, 1998; Tuch & Weitzer, 1997; Webb & Marshall, 1995; Weitzer, 2000; Tomaskovic-Devey et al., 2004; Cao et al., 1996; Huang & Vaughn, 1996
[44] Apple & O'Brien, 1983; Thomas & Hyman, 1977; Boggs & Galiher, 1965; Winfree & Griffiths, 1977; Hurst & Frank, 2000

Appendix B: References

APPENDIX B: REFERENCES

Alpert, G. P. (1989). Police use of deadly force: The Miami experience. *Critical issues in policing*, 480-496.

Apple, N., & O'Brien, D. (1983). Neighborhood racial composition and residents' evaluation of police performance. *Journal of Police Science and Administration*, *11*(1), 76-84.

Ariel, B. (2016a). Police body cameras in large police departments. *The Journal of Criminal Law and Criminology*,106, 729–768.

Ariel, B. (2016b). Increasing cooperation with the police using body-worn cameras. *Police Quarterly*, 19, 326–362

Ariel, B., Farrar, W. A., & Sutherland, A. (2015). The effect of police body-worn cameras on use of force and citizens' complaints against the police: A randomized controlled trial. *Journal of Quantitative Criminology*, 31, 509–535.

Ariel, B., Sutherland, A., Henstock, D., Young, J., Drover, P., Sykes, J., Henderson, R. (2016a). Report: Increases in police use of force in the presence of body-worn cameras are driven by officer discretion: A protocol based subgroup analysis of ten randomized experiments. *Journal of Experimental Criminology*, 12, 453–463.

Ariel, B., Sutherland, A., Henstock, D., Young, J., Drover, P., Sykes, J., Henderson, R. (2016b). Wearing body cameras increases assaults against officers and does not reduce police use of force: Results from a global multi-site experiment. *European Journal of Criminology*, 13, 744–755.

Ariel, B., Sutherland, A., Henstock, D., Young, J., Drover, P., Sykes, J., Henderson, R. (2017). "Contagious account-ability": A global multisite randomized controlled trial on the effect of police body-worn cameras on citizens' com-plaints against the police. *Criminal Justice and Behavior*, 44, 293–316.

Ariel, B., Sutherland, A., Henstock, D., Young, J., Drover, P., Sykes, J., Henderson, R. (2018). Paradoxical effects of self-awareness of being observed: Testing the effect of police body-worn cameras on assaults and aggression against officers. *Journal of Experimental Criminology*, 14, 19–47

Boggs, S.L. and Galliher, S.F. (1965), "Evaluating the Police: A Comparison of Black Street and Household Respondents", *Social Problems*, 13:393-406.

Braga, A. A., Barao, L., McDevitt, J., & Zimmerman, G. (2018a). *The impact of body-worn cameras on complaints against officers and officer use of force incident reports: Preliminary evaluation findings*. Boston, MA: Northeastern University Press.

Braga, A. A., Sousa, W. H., Coldren, J. R., Jr., & Rodriguez, D. (2018b). The effects of body-worn cameras on police activity and police-citizen encounters: A randomized controlled trial. *Journal of Criminal Law and Criminology*,108, 511–538.

Braga, A., Coldren, J., Sousa, W., Rodriguez, D. and Alper, O. (2017). "The Benefits of Body-Worn Cameras: New Findings from a Randomized Controlled Trial at the Las Vegas Metropolitan Police Department." Final report to the National Institute of Justice.

Brooks, L. W. (2001). Police discretionary behavior: A study of style. *Critical issues in policing: Contemporary readings*, 71-131.

Brown, R. A., & Frank, J. (2006). Race and officer decision making: Examining differences in arrest outcomes between black and white officers. *Justice quarterly*, *23*(1), 96-126.

Cao, L., Frank, J., & Cullen, F. T. (1996). Race, community context and confidence in the police. *American Journal of Police*, 15(1), 3-22.

Decker, S. H. (1981). Citizen attitudes toward the police: A review of past findings and suggestions for future policy. *Journal of police science and administration*, *9*(1), 80-87.

DiGangi, D. (2019, January 24). Virginia lawmakers want to stop spoofed robocalls. Retrieved June 28, 2019, from https://wjla.com/news/local/virginia-lawmakers-want-to-stop-spoofed-robocalls

Edmonton Police Service [Mary Stratton, Peter Clissold, and Rick Tuson]. (2015). *Body-worn video: Considering the evidence: Final report of the Edmonton police service body-worn video pilot project.* Edmonton, AB, Canada: Edmonton Police Service. Retrieved from https://bwvsg.com/wp-content/uploads/2015/06/Edmonton-Police-BWV-Final-Report.pdf

Ellis, T., Jenkins, C., & Smith, P. (2015). *Evaluation of the introduction of personal issue body-worn video cameras (Operation Hyperion) on the Isle of Wight: Final report to Hampshire constabulatory.* Portsmouth, England: Institute of Criminal Justice Studies, University of Portsmouth. Retrieved from http://www2.port.ac.uk/media/contacts-and-departments/icjs/downloads/Ellis-Evaluation-Worn-Cameras.pdf

Engel, R. S., & Worden, R. E. (2003). Police Officers' Attitudes, Behavior, and Supervisory Influences: an Analysis of Problem Solving. *Criminology*, *41*(1), 131-166.

Ernest-Jones, M., Nettle, D., & Bateson, M. (2011). Effects of eye images on everyday cooperative behavior: a field experiment. *Evolution and Human Behavior*, 32(3), 172-178.

Fyfe, J. J. (1988). Police use of deadly force: Research and reform. *Justice quarterly*, *5*(2), 165-205.

Gallagher, C., Mastrofski, S. D., Maguire, E., & Reisig, M. D. (2001). The public image of the police.

Gaub, J. E., Choate, D. E., Todak, N., Katz, C. N., & White, M. D. (2016). Officer perceptions of body-worn cameras before and after deployment: A study of three departments. *Police Quarterly*, 19, 275–302.

Gaub, J. E., Todak, N., & White, M. D. (2018). One size doesn't fit all: The deployment of police body-worn cameras to specialty units. *International Criminal Justice Review*, 1057567718789237.

Goodall, M. (2007). *Guidance for the police use of body-worn video devices: Police and crime standards directorate.* London, U.K.: Home Office. Retrieved from https://library.college.police.uk/docs/homeoffice/guidance-body-worn-devices.pdf

Gramagila, J. A., & Phillips, S. W. (2018). Police officers' perceptions of body-worn cameras in Buffalo and Rochester. *American Journal of Criminal Justice*, *43*(2), 313-328.

Grossmith, L., Owens, C., Finn, W., Mann, D., Davies, T., & Baika, L. (2015). Police, camera, evidence: London's cluster randomised controlled trial of body-worn video. *London: College of Policing*.

Headley, A. M., Guerette, R. T., & Shariati, A. (2017). A field experiment of the impact of body-worn cameras (BWCs) on police officer behavior and perceptions. *Journal of Criminal Justice*, 53, 102-109.

Hedberg, E. C., Katz, C. M., & Choate, D. E. (2017). Body-worn cameras and citizen interactions with police officers: Estimating plausible effects given varying compliance levels. *Justice quarterly*, *34*(4), 627-651.

Hinds, L. and Murphy, K. (2007). Public satisfaction with police: Using procedural justice to improve police legitimacy. *Australian & New Zealand Journal of Criminology* 40:27–42

Huang, W., & Vaughn, M. (1996). Support and confidence: Public attitudes toward the police. *Americans view crime and justice: A national public opinion survey*, 31-45.

Hurst, Y. G., & Frank, J. (2000). How kids view cops The nature of juvenile attitudes toward the police. *Journal of criminal justice*, *28*(3), 189-202.

Hyland, S. S. (2018). Body-worn cameras in law enforcement agencies, 2016. Washington, DC: U.S. Department of Justice, Office of Justice Programs, Bureau of Justice Statistics.

Hyland, S. S. (2018). *Body-worn Cameras in Law Enforcement Agencies, 2016*. Washington, DC: Office of Justice Programs, Bureau of Justice Statistics. Retrieved from https://www.bjs.gov/content/pub/pdf/bwclea16.pdf

Jackson, J., Bradford, B., Hough, M., Myhill, A., Quinton, P., & Tyler, T. R. (2012). Why do people comply with the law? Legitimacy and the influence of legal institutions. *British journal of criminology*, *52*(6), 1051-1071.

Jennings, W. G., Fridell, L. A., & Lynch, M. D. (2014). Cops and cameras: Officer perceptions of the use of body-worn cameras in law enforcement. *Journal of Criminal Justice*, 22, 549–556.

Jennings, W. G., Lynch, M. D., & Fridell, L. A. (2015). Evaluating the impact of police officer body-worn cameras (BWCs) on response-to-resistance and serious external complaints: Evidence from the Orlando police department (OPD) experience utilizing a randomized controlled experiment. *Journal of Criminal Justice*, 43, 480–486.

Johnson, D., Maguire, E. R., & Kuhns, J. B. (2014). Public Perceptions of the Legitimacy of the Law and Legal Authorities: Evidence from the Caribbean. *Law & Society Review*, *48*(4), 947-978.

Katz, C. M., Choate, D. E., Ready, J. R., & Nuño, L. (2014). Evaluating the impact of officer worn body cameras in the Phoenix police department. *Phoenix, AZ: Center for Violence Prevention & Community Safety, Arizona State University*.

Kyle, M. J., & White, D. R. (2017). The impact of law enforcement officer perceptions of organizational justice on their attitudes regarding body-worn cameras. *Journal of Crime and Justice*, 40(1), 68-83.

Linden, A. (2015). Conducting interrupted time-series analysis for single-and multiple-group comparisons. *The Stata Journal*, *15*(2), 480-500.

Lum, C., Stoltz, M., Koper, C. S., & Scherer, J. A. (2019). Research on body-worn cameras: What we know, what we need to know. *Criminology & Public Policy*, *18*(1), 93-118.

Maskaly, J., Donner, C., Jennings, W. G., Ariel, B., & Sutherland, A. (2017). The effects of body-worn cameras (BWCs) on police and citizen outcomes: A state-of-the-art review. *Policing: An International Journal of Police Strategies & Management*, 40, 672–688.

Mastrofski, S. D., Snipes, J. B., & Supina, A. E. (1996). Compliance on demand: The public's response to specific police requests. *Journal of Research in Crime and Delinquency*, 33(3), 269-305.

Mazerolle, L., Antrobus, E., Bennett, S., & Tyler, T. R. (2013). Shaping citizen perceptions of police legitimacy: A randomized field trial of procedural justice. *Criminology*, *51*(1), 33-63.

McClure, D., La Vigne, N., Lynch, M., Golian, L., Lawrence, D., & Malm, A. (2017). How body cameras affect community members' perceptions of police. *Results from a randomized controlled trial of one agency's pilot. Washington, DC: Urban Institute*.

McCluskey, J. D. (2003). *Police requests for compliance: Coercive and procedurally just tactics*. LFB Scholarly Pub..

McCluskey, J. D., Uchida, C. D., Solomon, S. E., Wooditch, A., Connor, C., & Revier, L. (2019). Assessing the effects of body-worn cameras on procedural justice in the Los Angeles Police Department. *Criminology*, 57(2), 208-236.

Morrow, W. J., Katz, C. M., & Choate, D. E. (2016). Assessing the impact of body-worn cameras on arresting, prose-cuting, and convicting suspects of intimate partner violence. *Police Quarterly*, 19, 303–325

Munger, K., & Harris, S. J. (1989). Effects of an observer on handwashing in a public restroom. *Perceptual and Motor Skills*, *69*(3-1), 733-734.

ODS Consulting [Andrew Fyfe]. (2011). *Body-worn video projects in Paisley and Aberdeen, self evaluation.* Retrieved from https://bwvsg.com/wp-content/uploads/2013/07/BWV-Scottish-Report.pdf

Owens, C., Mann, D., & Mckenna, R. (2014).*The Essex body-worn video trial: The impact of body-worn video on criminal justice outcomes of domestic abuse incidents*. Ryton-on-Dunsmore, Coventry, England: College of Policing. Retrieved from https://bwvsg.com/wp-content/uploads/2013/07/BWV_ReportEssTrial.pdf

Paoline, E.A. (2001), "Rethinking police culture: officers' occupational attitudes", LFB Scholarly Publishing, LLC, New York, NY.

Ratcliffe, J. H., Taniguchi, T., & Taylor, R. B. (2009). The crime reduction effects of public CCTV cameras: a multi-method spatial approach. *Justice Quarterly*, *26*(4), 746-770.

Reisig, M. D., & Parks, R. B. (2000). Experience, quality of life, and neighborhood context: A hierarchical analysis of satisfaction with police. *Justice Quarterly*, *17*(3), 607-630.

Reiss, A. J. (1971). *The police and the public* (Vol. 39). Yale University Press.

Sampson, R. J., & Bartusch, D. J. (1998). Legal cynicism and (subcultural) tolerance of deviance: the neighborhood context of racial difference. *Law & Society Rev.*, *32*, 777.

Scaglion, R., & Condon, R. G. (1980). Determinants of Attitudes Toward City Police. *Criminology*, *17*(4), 485-494.

Sherman, L. W. (1978). *Scandal and reform: Controlling police corruption*. Univ of California Press.

Smith, D. A., & Klein, J. R. (1983). Police agency characteristics and arrest decisions. *Evaluating performance of criminal justice agencies*, *19*, 63-98.

Smith, P. E., & Hawkins, R. O. (1973). Victimization, types of citizen-police contacts, and attitudes toward the police. *Law & Soc'y Rev.*, *8*, 135.

Sousa, W. H., Miethe, T. D., & Sakiyama, M. (2018). Inconsistencies in public opinion of body-worn cameras on police: Transparency, trust, and improved police–citizen relationships. *Policing: A Journal of Policy and Practice*, 12, 100–108.

Sousa, W.H., Miethe, T.D. and Sakiyama, M. (2015), "Research in Brief: Body-Worn Cameras on Police: Results from a National Survey of Public Attitudes." Center for Crime and Justice Policy, University of Nevada – Las Vegas, Las Vegas, NV

Sun, I. Y., & Payne, B. K. (2004). Racial differences in resolving conflicts: A comparison between Black and White police officers. *Crime & delinquency*, *50*(4), 516-541.

Sunshine, J., & Tyler, T. R. (2003). The role of procedural justice and legitimacy in shaping public support for policing. *Law & society review*, *37*(3), 513-548.

Tankebe, J. (2013). Viewing things differently: The dimensions of public perceptions of police legitimacy. *Criminology*, *51*(1), 103-135.

Telep, C. W. (2017). Police officer receptivity to research and evidence-based policing: examining variability within and across agencies. *Crime & delinquency*, *63*(8), 976-999.

Terrill, W., & Reisig, M. D. (2003). Neighborhood context and police use of force. *Journal of research in crime and delinquency*, *40*(3), 291-321.

Thomas, C. W., & Hyman, J. M. (1977). Perceptions of crime, fear of victimization, and public perceptions of police performance. *Journal of police science and administration*, *5*(3), 305-317.

Tomaskovic- Tomaskovic-Devey, D., Mason, M., & Zingraff, M. (2004). Looking for the driving while black phenomena: Conceptualizing racial bias processes and their associated distributions. *Police Quarterly*, *7*(1), 3-29.

Toronto Police Service. (2016). Body-worn cameras: *A report on the findings of the pilot project to test the value and feasibility of body-worn cameras for police officers in Toronto*. Toronto, ON, Canada: Author.

Tuch, S. A., & Weitzer, R. (1997). The polls--trends: Racial differences in attitudes toward the police. *Public opinion quarterly*, *61*(4), 642.

Tyler, T. R. (1988). What is procedural justice-criteria used by citizens to assess the fairness of legal procedures. *Law & Soc'y Rev.*, *22*, 103.

Tyler, T. R. (2004). Enhancing police legitimacy. *The annals of the American academy of political and social science*, *593*(1), 84-99.

Tyler, T. R. (2006). *Why people obey the law*. Princeton University Press.

Tyler, T. R., & Fagan, J. (2008). Legitimacy and cooperation: Why do people help the police fight crime in their communities. *Ohio St. J. Crim. L.*, *6*, 231.

Tyler, T.R. and Huo, Y.J. (2002), *Trust In the Law: Encouraging Public Cooperation with the Police and Courts*. Russell Sage, New York, NY.

Wahl, G. M., Islam, T., Gardner, B., Marr, A. B., Hunt, J. P., McSwain, N. E., ... & Duchesne, J. (2010). Red light cameras: do they change driver behavior and reduce accidents?. *Journal of Trauma and Acute Care Surgery*, *68*(3), 515-518.

Wallace, D., White, M. D., Gaub, J. E., & Todak, N. (2018). Body - worn cameras as a potential source of depolicing: Testing for camera - induced passivity. *Criminology*, 56(3), 481-509.

Webb, V. J., & Marshall, C. E. (1995). The relative importance of race and ethnicity on citizen attitudes toward the police. *American Journal of Police*, *14*(2), 45-66.

Weitzer, R. (2000). White, black, or blue cops? Race and citizen assessments of police officers. *Journal of Criminal Justice*, *28*(4), 313-324.

Wells, W. (2007). Type of contact and evaluations of police officers: The effects of procedural justice across three types of police–citizen contacts. *Journal of Criminal Justice*, *35*(6), 612-621.

White, M. D., Gaub, J. E., & Todak, N. (2018a). Exploring the potential for body-worn cameras to reduce violence in police-citizen encounters. *Policing: A Journal of Policy and Practice*, 12, 66–76.

White, M. D., Todak, N., & Gaub, J. E. (2017). Assessing citizen perceptions of body-worn cameras after encounters with police. *Policing: An International Journal of Police Strategies and Management*, 40, 689–703.

White, M. D., Todak, N., & Gaub, J. E. (2018b). Examining body-worn camera integration and acceptance among police officers, citizens, and external stakeholders. *Criminology & Public Policy*, 17, 649–677.

Wicklund, R. A. (1975). Objective self-awareness. In *Advances in experimental social psychology* (Vol. 8, pp. 233-275). Academic Press.

Winfree, T., & Griffiths, C. (1977). Adolescent attitudes toward the police. *Juvenile delinquency: Little brother grows up*, *2*, 79-99.

Worden, R. E. (1989). Situational and attitudinal explanations of police behavior: A theoretical reappraisal and empirical assessment. *Law and Society Review*, 667-711.

Yokum, D., Ravishankar, A., and Coppock, A. (2017). *Evaluating the Effects of Police Body-Worn Cameras: A Randomized Controlled Trial*. Washington, DC: The Lab@DC. Retrieved from http://bwc.thelab.dc.gov/TheLabDC_MPD_BWC_Working_Paper_10.20.17.pdf

Appendix C: Stakeholder Survey

POLICE OFFICER BODY-WORN CAMERA STUDY, FAIRFAX, VIRGINIA

STAKEHOLDER SURVEY INSTRUMENT

Developed by
Richard Bennett, Ph.D.
Brad Bartholomew, Ph.D.

Contents

INFORMED CONSENT

Consent to Participate in an Online Survey

You are being asked to participate in an online survey. It is part of a larger research study being conducted by Prof. Richard Bennett and Prof. Bard Bartholomew from American University in Washington, DC. The study is evaluating the effectiveness of Body-Worn Camera (BWC) Pilot Program by the Fairfax County Police Department (FCPD).

Research Procedures

If you agree to participate in this study, you will be asked about your attitudes towards the use of body-worn cameras in your community and its potential effect on policing in your community. You will also be asked about your knowledge of the FCPD and its BWC program. The survey will take 10-15 minutes to complete. All responses are anonymous and no information about you or your computer will be collected. All data collected during the study will be stored in a secure place, accessible only by the researchers, for future analysis. The Fairfax County Police will never know how you answered these questions.

Risks and Benefits

Your participation involves no more than minimal risks to you. There may be benefits to you and your community by participating. The findings of this survey will be reported to the FCPD and might be used to change the type and extent of police services delivered to your community. Overall, the study will contribute to our general knowledge about the effectiveness of using BWCs.

Your Participation

Your participation in the survey is entirely voluntary. You may choose not to answer specific questions or to exit from the survey at any point, without consequences of any kind.

Questions about the Study?

If you have questions about the study, please feel free at any time to contact Prof. Brad Bartholomew at (Bartholo@american.edu or 443-812-4616). If you have questions about your rights as a research subject, please contact Matt Zembrzuski, IRB Coordinator at American University via email at irb@american.edu or by phone at (202) 885-3447.

Giving of Consent

By taking the survey, you are indicating that you have read and understood this consent form and agree to participate in this research study.

[EFFECTS OF BODY-WORN CAMERAS]

When answering the following questions, please do so in your role as a stakeholder in the community. That is, how would members of your organization answer these questions. There are no right or wrong answers. Please answer the following questions by checking the appropriate box using a five-point scale ranging from of Strongly Agree to strongly disagree**.**

	STRONGLY AGREE	AGREE	DISAGREE	STRONGLY DISAGREE	DON'T KNOW
1. The police will be more respectful to citizens when wearing a video camera.	1	2	3	4	-8
2. Citizens will be more cooperative when they become aware that an officer is wearing a video camera.	1	2	3	4	-8
3. For the BWC to work, the community must be made aware of their use.	1	2	3	4	-8
4. People will feel safer knowing that the police are wearing a video camera.	1	2	3	4	-8
5. The use of video cameras will reduce complaints against the police.	1	2	3	4	-8
6. The BWC program will make the police more accountable.	1	2	3	4	-8
7. The BWC program will make the police more transparent.	1	2	3	4	-8
8. The BWC program will make the police more legitimate in the eyes of my community.	1	2	3	4	-8
9. The use of video cameras will help citizens resolve complaints against the police.	1	2	3	4	-8
10. The use of video cameras will lower the amount of force used by the police in encounters with citizens.					
11. The use of video cameras will lower the number of police imitated encounters with citizens.					

[OPINIONS ON FAIRFAX COUNTY POLICE DEPARTMENT]

The following questions are about your opinions about The Fairfax County Police Department. There are no right or wrong answers. Please answer the following questions by checking the appropriate box using a five-point scale ranging from of Strongly Agree to strongly disagree

	STRONGLY AGREE	AGREE	DISAGREE	STRONGLY DISAGREE	DON'T KNOW
12. As a community stakeholder, I believe that I was adequately involved in the development of the BWC policy.	1	2	3	4	-8
13. As a community stakeholder, I believe that my concerns about the BWC program were adequately heard by the FCPD.	1	2	3	4	-8
14. The Fairfax County Police Department shares the values of my community.	1	2	3	4	-8
15. The Fairfax County Police Department does its job well.	1	2	3	4	-8
16. The Fairfax County Police Department is effective at preventing crime.	1	2	3	4	-8
17. The Fairfax County Police Department is effective in solving crimes and arresting perpetrators.	1	2	3	4	-8

18. Have you read the Fairfax County Police BWC policy?

YES _____, NO _____ (GO TO 16)

19. In your opinion, what is the most important benefit and drawback of the Fairfax County Police BWC policy?

What is the most important benefit?

What is the most important drawback?

20. Have you talked with members of your community about the BWC program?

YES _____, NO_____

21. If yes, what was their reaction to the BWC program?

22. If no, do you plan on talking with your community members about the BWC program in the future?

YES _____, NO_____, DON"T KNOW_____

23. What are your suggestions for improving the services you and your community receive from the Fairfax County Police?

Organizational Indicators

24. What is the name of the organization you represent?

25. What do you see as its role in the community?

26. How long have you represented this organization?

27. What is your leadership role in it?

Appendix D:
Fairfax County Police Officer Survey

Fairfax County Police Officer Survey

Survey of Officers from the Mason, Mt. Vernon & Reston Districts

In partnership with American University, Department of Justice, Law and Criminology

AMERICAN UNIVERSITY
WASHINGTON, DC

Please note: Not $1 of Fairfax County money is being spent on this study. Financial support comes from American University and several foundations.

Consent to Participate in Research on Body-worn Cameras (BWCs)

You are being asked to participate in a research study conducted by faculty from American University in partnership with the FCPD. The purpose of the survey below is to understand your attitudes about the use of BWCs by police officers. This survey will take only 5 to 7 minutes of your time.

All of your responses will be kept strictly confidential and used only for research purposes. Your responses will never be seen by your commander or others in the FCPD. The department will only see the findings in aggregated form, as may other police agencies and individuals interested in the topic.

Your participation is voluntary. You are free to choose not to participate or to stop participating at any time without consequences. You may also decline to answer specific questions without consequences.

By filling out this survey, you are indicating that you have read and understood this consent form and agree to participate in the study.

If you have questions or concerns during the time of your participation in this study, or after its completion, please contact:

Prof. Richard Bennett
Department of Justice, Law and Criminology
American University. Bennett@american.edu, 202-885-2956

If you have questions about your rights as a research subject, please contact:
Matt Zembrzuski
IRB Coordinator
American University. irb@american.edu, 202-885-3447

The Fairfax County Police Department has formed a partnership with American University to study officers' attitudes toward police use of body-worn cameras (or BWCs) and their effects on contacts with citizens. This survey asks for your opinions about the use and effectiveness of BWCs in police work.

Your honest opinions and perceptions are important to our research team. Please circle the number that best represents your feelings about each statement.

	Strongly Disagree			Unsure			Strongly Agree
Citizen Behavior --- ***When BWCs are in use***	↓			↓			↓
1. Relations between police and the public will improve.	1	2	3	4	5	6	7
2. Suspects will be less likely to resist arrest.	1	2	3	4	5	6	7
3. Citizens will be less cooperative.	1	2	3	4	5	6	7
4. Citizens will become more respectful.	1	2	3	4	5	6	7
5. The number of citizen complaints against officers will increase.	1	2	3	4	5	6	7
6. Citizens will be more likely to view the police as legitimate enforcers of the law.	1	2	3	4	5	6	7
Police Officer Behavior --- ***When wearing a BWC, officers will:***							
7. Act more professionally.	1	2	3	4	5	6	7
8. Respond more slowly to calls for service.	1	2	3	4	5	6	7

	Strongly Disagree			Unsure			Strongly Agree
9. Be less proactive when it comes to engaging with citizens.	1	2	3	4	5	6	7
10. Be less likely to use force when engaging with citizens.	1	2	3	4	5	6	7
11. Have fewer contacts with citizens.	1	2	3	4	5	6	7
12. Be less likely to give warnings to citizens.	1	2	3	4	5	6	7
13. Feel they have less discretion.	1	2	3	4	5	6	7
14. Find ways to avoid/subvert BWC policy	1	2	3	4	5	6	7
15. Be upset if not selected to wear a camera	1	2	3	4	5	6	7
Evidence---*The use of BWCs will help to:*							
16. Gather evidence	1	2	3	4	5	6	7
17. Identify criminal suspects	1	2	3	4	5	6	7
18. Increase likelihood of conviction	1	2	3	4	5	6	7
19. Settle complaints about an officer's behavior when interacting with a citizen.	1	2	3	4	5	6	7
General Perceptions --- *The use of BWCs will:*							
20. Increase officer safety	1	2	3	4	5	6	7
21. Reduce crime	1	2	3	4	5	6	7

	Strongly Disagree			Unsure			Strongly Agree
22. Increase the transparency of the department to itself.	1	2	3	4	5	6	7
23. Increase the transparency of the department to the public.	1	2	3	4	5	6	7
24. Improve the overall job performance of an officer.	1	2	3	4	5	6	7
25. A major reason for the use of BWCs is so supervisors can more closely monitor, control and sanction officers under them.	1	2	3	4	5	6	7
26. Get in the way of an officer's routine actions/movement.	1	2	3	4	5	6	7
Overall Recommendations:							
27. Even though officer-citizen interactions are currently recorded by in car video, there will be significant resistance by officers to the use of BWCs.	1	2	3	4	5	6	7
28. Fairfax County Police should adopt BWCs throughout the entire department.	1	2	3	4	5	6	7
29. The advantages of adopting BWCs outweighs the disadvantages.	1	2	3	4	5	6	7

For analysis purposes only, please answer these demographic questions. Again, your answers to this survey are strictly confidential and FCPD administrators will never see this instrument or the data it contains. Please place a **X** on the line that corresponds to your selection.

30. What is your current assignment?
    _____ A Squad
    _____ B Squad
    _____ Other

31. What is your patrol squad?
    _____ Days
    _____ Eves
    _____ Mids
    _____ NPU
    _____ Other Days
    _____ Other Eves

32. What is your current rank?
    _____ Officer (FCO, PFC, MPO)
    _____ First Line Supervisor (SGT, 2nd LT.)
    _____ Other

33. How many years of police experience do you have?
    _____ (If less than a year, insert a zero)

34. What is your gender?
    _____ Male
    _____ Female
    _____ Transgender, other

35. Which racial category describes you best?

_____ African-American
_____ Asian/Pacific Islander
_____ Caucasian, White
_____ Hispanic
_____ Native American
_____ Other/Multiple

36. What is the highest level of school you have completed?

_____ High school diploma/GED
_____ Some college
_____ Two-year degree
_____ Four-year degree
_____ Advanced degree

37. The BWC pilot program will last for six months. What one or two things should the department do, not do or watch out for so that the pilot program that might undermine the integrity of it?

38. Finally, is there anything that we did not ask but you think is important for us to know?

Please fold and insert this survey in the locked box labeled “Fairfax County Police Department Officer Survey.”

Thank you very much for participating in this important study.

Appendix E:
Community Member Telephone Survey

POLICE OFFICER BODY-WORN CAMERA STUDY, FAIRFAX, VIRGINIA

RESIDENT TELEPHONE SURVEY INSTRUMENT

Developed by
Richard Bennett, Ph.D.
Brad Bartholomew, Ph.D.

Contents

Text on Card Handed-out for FCPD Officers:

Face of Card (size of business card):

The American University in Partnership with the Fairfax County Police Department is evaluating their Body-Worn Camera Pilot Program. The officer handing you this card is part of the program. We, at American University, might be calling you next week about your experiences.

PLEASE KEEP THIS CARD

Reverse of Card:

Your responses to the survey will be held in the strictest confidence and **the officer and the department will never know what you said.** We hope you will cooperate with the researchers at American University. If you would like to know more about the survey, please contact Dr. Brad Bartholomew at 202-885-2367 at the American University in Washington, DC.

Introduction and Informed Consent:

Hi, my name is [INTERVIEWER'S FULL NAME] and I'm calling from the American University in Washington, DC. I'm talking with residents who had recent contact with the Fairfax County police. The survey will only take 5 minutes of your time.

IF NO... Is there a good time for me to call you back? We are hoping to obtain your feedback to improve police interactions with the public and your participation in the survey would be really helpful.

IF YES... Thank you. The survey will be used to improve police interactions with the public. The survey is completely voluntary, and you may stop at any time or skip any questions you don't want to answer. Everything you say will be kept confidential and used only for research purposes. Additionally, your name will never be associated with any of your answers and the Fairfax County Police Department will never know how you answered this survey. By beginning the survey, you have understood the above and are willing to participate. Do you have any questions?

i. Are you at least 18 years old?

YES..... 1

NO 0

Don't KNOW..... -8

REFUSED..... -9

ii. Were you directly involved in a recent encounter with the police?

YES..... 1 (SKIP TO Q1)

NO 0

DON'T KNOW ..... -8

REFUSED..... -9

iii. Could I please speak with a member of this household who was involved in this encounter?

YES..... 1 (GO TO iv)

NO ..... 0 (THANK YOU AND GOOD BYE)

DON'T KNOW ..... -8

REFUSED..... -9

iv. When person involved in incident picks up the phone, go back and redo introduction and informed consent. And repeat questions i & ii.

[SATISFACTION WITH POLICE ENCOUNTER]

The following questions are about your recent contact with Fairfax County Police on (Date). There are no right or wrong answers. Your opinions and personal experiences are important to us. Please tell me if you strongly agree, agree, disagree, strongly disagree or Don't know to the following statements.

	STRONGLY AGREE	AGREE	DISAGREE	STRONGLY DISAGREE	DON'T KNOW	REFUSED
The police officer I spoke with treated you with respect.	1	2	3	4	-8	-9
2. The officer treated me fairly.	1	2	3	4	-8	-9
3. The officer explained his or her actions and decisions to me during our interaction.	1	2	3	4	-8	-9
4. The officer listened carefully to what I had to say.	1	2	3	4	-8	-9
5. The officer acted professionally.	1	2	3	4	-8	-9
6. The officer cared about my well-being.	1	2	3	4	-8	-9
7. I am satisfied with how I was treated by the police.	1	2	3	4	-8	-9
8. I am satisfied with how my situation was resolved.	1	2	3	4	-8	-9
9. I believe that the police share the values of my community?	1	2	3	4	-8	-9
10. I believe that the Fairfax County Police Department does its job well.	1	2	3	4	-8	-9
11. I believe that the Fairfax County Police Department is effective at preventing crime.	1	2	3	4	-8	-9

12. Was the officer you had the most contact with

Male 0

Female 1

DON'T KNOW ..... -8

REFUSED..... -9

13. Would you best describe the officer as

White 1

Black 2

Hispanic 3

Asian 4

Other 5

DON'T KNOW ..... -8

REFUSED ..... -9

I will now ask you questions and you can answer either yes or no.

	YES	NO	DON'T KNOW	REFUSED
14. During the encounter, did the officer use or threaten to use force?	1	0	-8	-9
15. Were you injured as a result of this incident?	1	0	-8	-9
16. To the best of your knowledge, were any of the officers wearing a video camera? (IF NO, GO TO Q29)	1	0	-8	-9

17. How did you know the officer was wearing a video camera?

THE OFFICER TOLD YOU AT THE TIME 1

YOU NOTICED THE CAMERA ON YOUR OWN 2

THROUGH A FORMAL PROCESS SUCH AS A PUBLIC RECORDS REQUEST OR COURT HEARING 3

Other 4

DON'T KNOW ..... -8

Refused ..... -9

[IMPACT ON BEHAVIOR]

18. Do you think the video camera influenced how you reacted to the police?

YES.....1

NO 0

DON'T KNOW .....-8

REFUSED.....-9

19. Did the video camera influence how the police reacted to you?

YES.....1

NO 0

DON'T KNOW..... -8

REFUSED.....-9

I am interested in how the video camera that the officer was wearing made you feel while you were interacting with the police. Tell me if you **strongly agree**, **agree**, **disagree** or **strongly disagree** with the following statements.

	STRONGLY AGREE	AGREE	DISAGREE	STRONGLY DISAGREE	DON'T KNOW	REFUSED
20. You felt safer knowing that the police were wearing video cameras.	1	2	3	4	-8	-9
21. The video camera made you uncomfortable.	1	2	3	4	-8	-9
22. You were more cooperative because the camera was on.	1	2	3	4	-8	-9
23. You were more cautious about what you said or did in front of the officer.	1	2	3	4	-8	-9
24. You felt angry or annoyed that you were being recorded.	1	2	3	4	-8	-9

25. The video camera made you feel more confident in the police.	1	2	3	4	-8	-9
26. Citizens will be more cooperative when they become aware that an officer is wearing a video camera.	1	2	3	4	-8	-9
27. Police will be more respectful to citizens when wearing video cameras.	1	2	3	4	-8	-9

28. How safe do you feel walking alone during the day in your neighborhood?

Very Safe Somewhat safe Unsure Somewhat unsafe Very unsafe

29. How safe do you feel walking alone at night in your neighborhood?

Very Safe Somewhat safe Unsure Somewhat unsafe Very unsafe

29. What do you think the police should do to improve the services they offer your community?

[DEMOGRAPHIC INDICATORS]

30. Okay, now I'd like to finish up with a few questions about your background. In what year were you born?

_____

REFUSED.....-9

31. Would you best describe your gender identity as

Male, or.....0

Female?.....1

OTHER 3

REFUSED.....-9

32. Are you currently

Single (never married) 1

Married 2

Cohabitating..... 3

Divorced 4

Widowed, or 5

Separated? 6

REFUSED..... -9

33. How much education have you completed?

Some high school 1

High school diploma..... 2

Some college 3

Associate or Bachelor's degree, or 4

Graduate or Professional Degree 5

REFUSED..... -9

34. Would you best describe your race as

American Indian or Alaska native 1

Asian..... 2

Native Hawaiian or other Pacific Islander..... 3

Black or African American, or 4

White 5

REFUSED..... -9

35. In terms of your work situation, are you currently

Working full-time 1

Working part-time 2

Not working 3

Not working but enrolled in school full-time..... 4

Not working but disabled..... 5

Retired?..... 6

OTHER 7

REFUSED..... -9

36. How long have you lived at your current address? **[Fill in years and months]**

_____

DON'T KNOW ..... -8

REFUSED..... -9

At this point we are done with the survey. Do you have any questions for me? Okay, thank you for your time and cooperation. We really appreciate your participation in the study. Have a great _____.

Appendix F:
BWC Project: Moderator's Guide

BWC Project: Moderator's Guide (6.17.18)

1. Preliminaries
    a. Self-introduction by moderator and introduction of observer (Prof. Bartholomew from American University)
    b. Thank everyone for coming to the group
    c. Give brief description of how the focus group will be conducted
    d. Give purpose of this group: to learn about the attitudes and experiences of police officers like you on a variety of issues. This research is part of a larger project being conducted by American University, independently of the Fairfax County Police Department.
    e. Give ground rules:
        i. Everyone should speak so moderator will understand the range of attitudes and experiences among the participants, but of course when you speak is your choice.
        ii. Please: only one person speak at a time
        iii. For everyone to be comfortable speaking freely, group must agree that all comments made will not be shared outside the room.
        iv. After this group ends, only Prof. Bartholomew and I will analyze in what was said. That is our concern, not who said what. We'd like your permission to do an audio taping of this session for our analysis. As soon as the analysis is finished, the recording will be destroyed. I turned on the recorder several minutes ago so I could document what I just said. Do each of you agree to this session being recorded? (If a participant does not agree, excuse him/her from the group.)
        v. I'd like to begin with everyone introducing themselves. You know each other but we don't. Please state your just first name and your years of service as a Fairfax County police officer.

2. Thinking back, what was your first thought when you heard that the department was considering issuing body-worn cameras to its officers?

3. When you learned that your district would be one of only three to be issued cameras as part of an evaluation, what were your first thoughts?
    a. Did you think that police work in those districts would change? If so, in what ways?
        1. Did you expect changes in the behavior or attitudes of police officers?
        2. Did you expect changes in the behavior and attitudes of residents in the community?

4. When you learned that B Side officers like yourselves would be issued cameras, what were your first thoughts?
    a. Did you expect your own way of policing would change?
    b. Did you expect changes in the way residents would interact with you?

5. Have there in fact been changes, anticipated or not, in how you work and how residents interact with you?
    a. What has changed?
    b. How would you rate the changes you've seen on a 10-point scale where 1 = no changes to 10 = huge changes?

6. Do you think that the A Side officers in your district have changed their behavior over the months you've been using cameras?
    a. How about residents: do you think A Side officers have noticed changes in the attitudes or behavior of residents they encounter?

7. The chief and senior officers will soon decide whether to issue cameras to all officers. What advice would you offer them, based on your experience?
    a. Probe how implementation should be done.
    b. Probe how training should be done.
    c. Probe whether any changes in policy should be made.

8. Final question: should the department make a formal announcement to the public that it will or will not be issuing body-worn cameras to all officers, or not? Why do you recommend that?

9. Thank you so much for participating in this group. You have given me and the American University research team lots of insight into your experiences and concerns. Do you have any additional comments you want to make before this session ends? Thank you again.

Appendix G: Additional Figures

APPENDIX G: ADDITIONAL FIGURES

Figure G-1: Overall Traffic Stops for A and B Squads

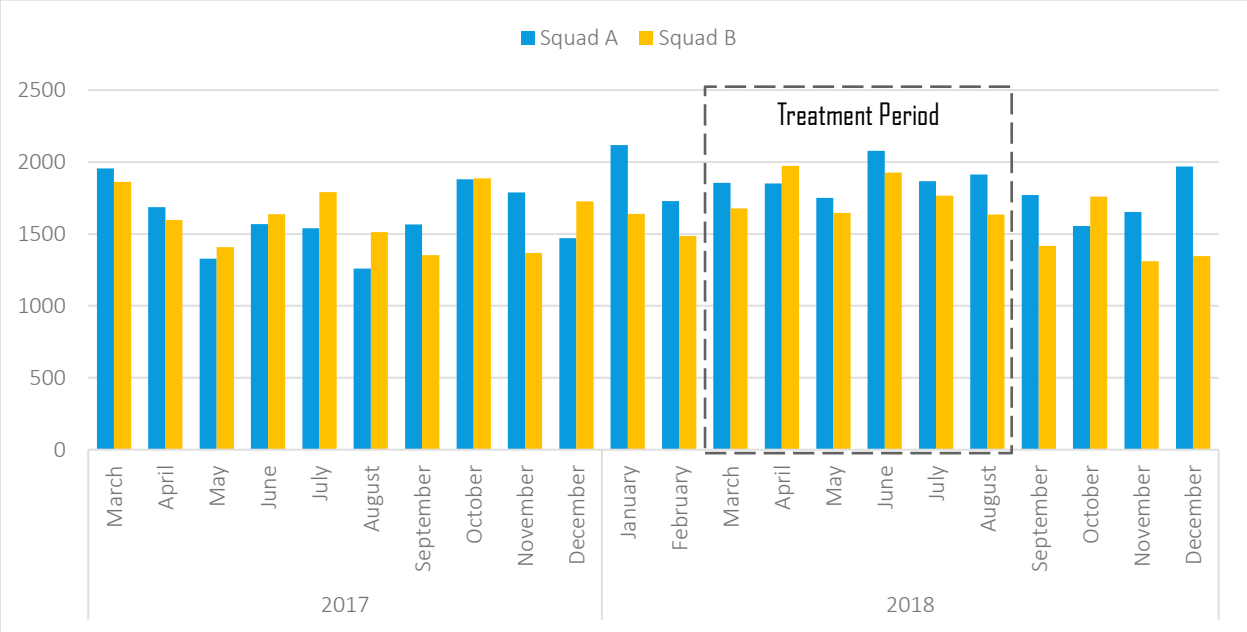


Figure G-2: Overall Incidents for A and B Squads

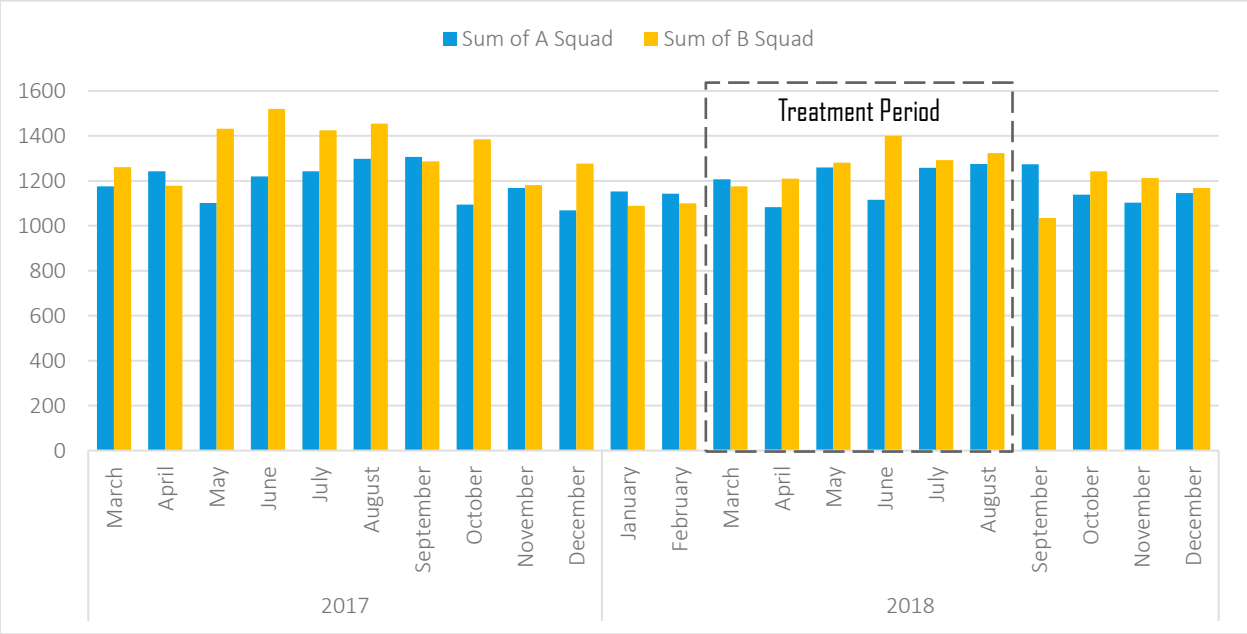


Figure G-3: Overall Citizen Complaints for A and B Squads

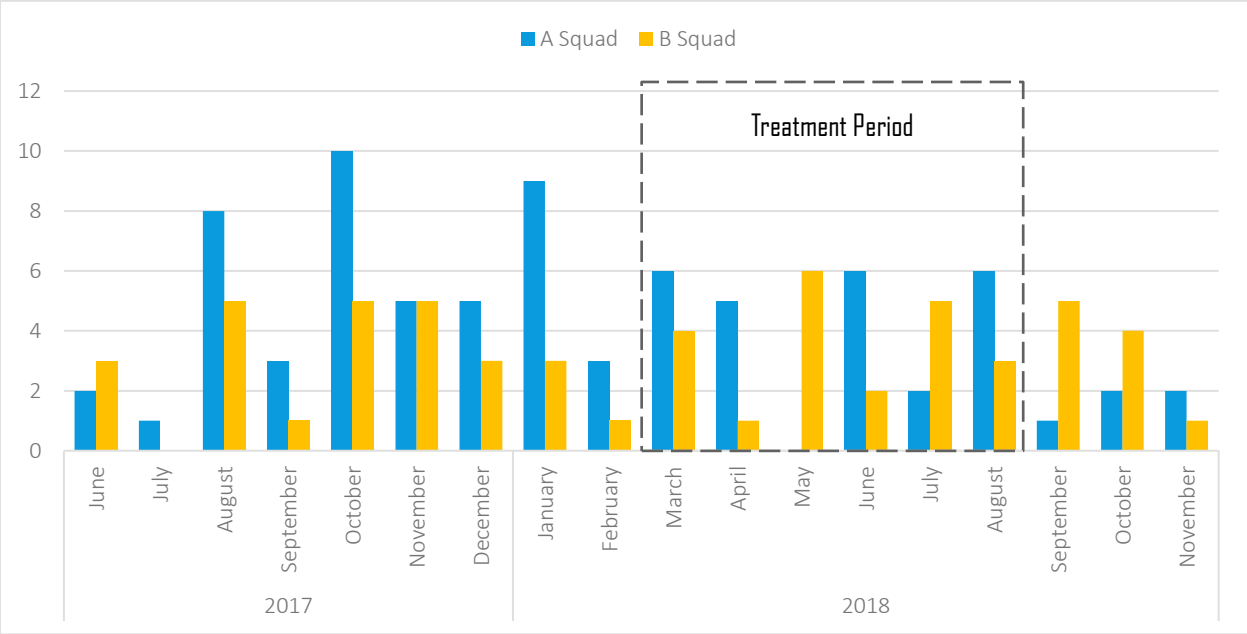
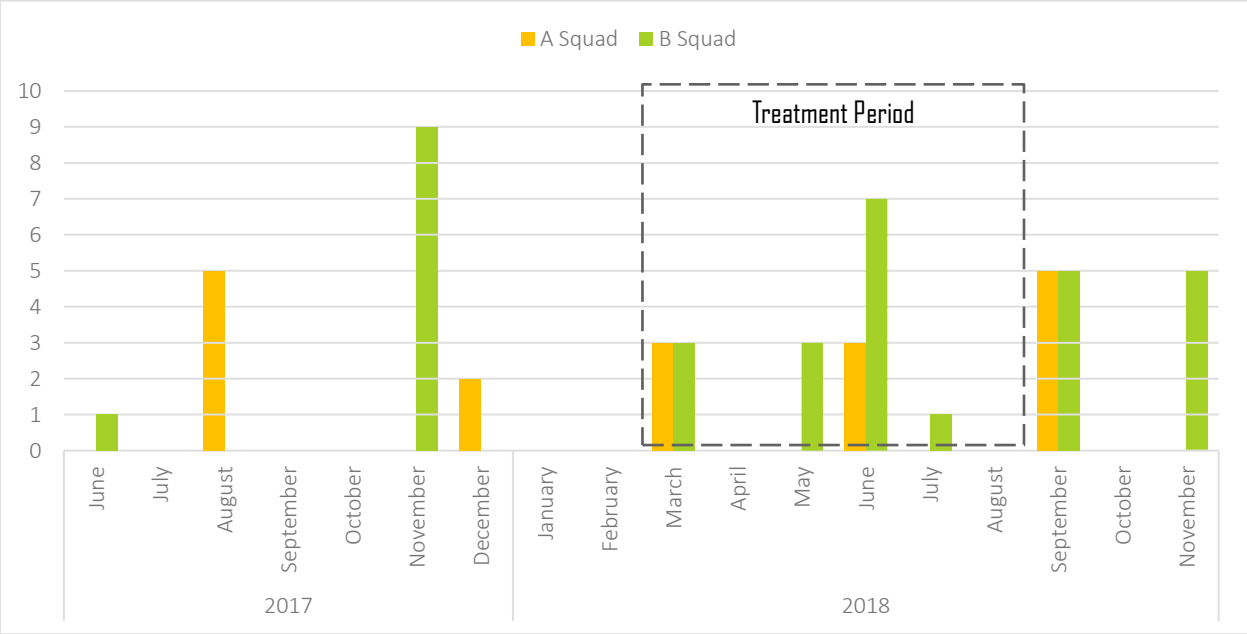


Figure G-4: Overall Use of Force Allegations for A and B Squads



Damon Mosler

Deputy District Attorney

Damon Mosler is the San Diego County Deputy District Attorney. He has been with the District Attorney's Office for over 27 years and is also currently the Chief of the Economic Crimes Division. He has served as Chief of both the Narcotics Division and Special Operations as well as a law enforcement liaison for the San Diego County Sheriff's Department. He has taught on a range of topics including: case preparation, predator/club drugs, informant handling, 4th amendment law and body worn camera concerns. He is a body worn camera subject matter expert for the Bureau of Justice Assistance and provides expertise and assistance to other district attorney's offices on data sharing, storage protocols, and legality issues pertaining to body worn camera policies.

Damon Mosler, Deputy District Attorney, San Diego County, California

Considerations and Impact of Body Worn Cameras on Prosecutors

Upon learning that a local law enforcement agency was preparing to deploy body-worn cameras (BWCs), we as prosecutors had to wonder what this new evidence would mean to our presentation of cases in court. Would it mean more or less work? More or fewer trials? Better trial outcomes?

In its simplest form, footage from BWCs could be considered just another type of evidence collected by law enforcement to prosecute offenders. But the novelty and volume of this type of media, as well as the public spotlight on it, makes the evidence unique. BWCs often capture more than officers can remember or more than they observed, which can pose testimonial concerns. Because officers cannot view all of their recordings before they write a report, some details that do not make it into a report may be called into question during testimony.

Given the reactive nature of law enforcement, what, if any, criminal activity would be caught on the BWC footage? And how will juries, judges, and the public react to criminal cases *without* video evidence? In light of the emerging nature of law enforcement's and prosecutors' experience with BWCs, it is important to give thought on the evidentiary nature of BWC footage as well as the impact the mass volume of data will have on the criminal justice system.

Crime Charging Expectations: As a practical matter, prosecutors cannot view all of the BWC evidence on a given case before making a charging decision. Even minor cases can generate several hours of video, especially if multiple videos of the same incident have been recorded. Charging prosecutors often have less than an hour to make a decision on whether to prosecute and what charges to file. With the advent of BWCs, many in law enforcement have voiced concerns that prosecutors will not file charges without video evidence. In fact, because most prosecutors assigned to review charges understand that crimes are rarely caught on camera, lack of video evidence should not pose a barrier to filing charges. Only certain crimes require BWC footage review prior to a charging decision: those involving force or violence against the officer or (in some instances) by the officer, those involving interaction with a mentally unbalanced person (to view the person's state of mind), domestic violence service calls (to hear and see the victim's report of the crime), and driving under the influence cases (to observe the impairment).

Courtroom Expectations: Without a doubt, as more BWCs are deployed, more videos will be used as evidence in court. And jurors, exposed to a barrage of outside media accounts in which crimes have been caught on video, will likely expect the crimes before them to be on video. By introducing some video in court, prosecutors can help manage those expectations. Yet, as most associated with police work know, the critical evidence in a case will not usually show up on BWC footage. As a practical matter, the videos are used more frequently to reflect what a victim, witness, or suspect said, and to assess the trustworthiness of those statements. Footage of an officer's initial contact with certain crime victims can serve as powerful and compelling evidence—much more so than a written report or in-court testimony months after an incident occurred. Prosecutors also rely on BWC footage to establish the on-scene true demeanor of the witnesses or suspects who testify about the events that occurred before the officers' arrival. Videos may also be used to help make a crime scene "come to life" through video captured by the first responding officers. Because BWC videos generally reflect well on police officers and help juries identify with officers, prosecutors are looking for ways to present videos to juries more often. In terms of courtroom presentation, it is incumbent on prosecutors to manage jury expectations of BWC tapes through jury selection questions, through the introduction of relevant tapes, and by direct examination of officers.

Courtroom Challenges: When and how BWCs get activated will also be a point of courtroom contention. A delayed activation or premature stoppage of the camera will generate questions and doubts. When events or statements are not caught on video, the officers may be subjected to more intense cross-examination, and their motives and professionalism may be called into question. Triers of fact must understand that the BWC does not follow the officer's eyes, so the officer can see things not on the video. Documentation and thorough reports will be critical. In addition, BWCs may capture more than the human eye can, and prosecutors may have to explain this in court. Because a BWC records in only two dimensions, it cannot capture the "speed of life" and seldom captures physiological cues given off in a contact. Prosecutors must work with testifying officers to explain to juries the limitations of BWCs in capturing the perspective, focus, history, and intent of the officer.

Evidentiary Matters: As with all evidence, how and when BWC recordings are received affects their ability to be used in court. Metadata labels, required on virtually all BWC recordings, provide sorting and organizing information and indicate the retention period for each video. Incorrectly categorized videos may be inadvertently purged by law enforcement before they are furnished to the prosecutor, resulting in missing evidence, which can imperil a prosecution. Late discovery of mislabeled videos can also delay a trial or limit admissibility, which could deprive the jury of relevant evidence that would paint a clearer picture of an event. Using the videos in court will require preparation of transcripts and, at times, redacted versions of the recording. Late rulings on what part of a video may be used and what must be excluded can also creating redaction and transcript difficulties that will limit videos from being used in certain cases.

Trial Preparation: To prepare effectively for court with BWC evidence, law enforcement officers and prosecutors will have to spend time together reviewing videos to ensure that proper questions are asked in court. Such preparation will also help when there are discrepancies between written reports and videos. Without a mutual understanding between officers and prosecutors of what is or is not on a video and why, presenting videos can open the door to unanswered questions and negatively affect a case.

Preservation and Storage of Video Evidence: Which recordings will be retained after disposition of the case? All recordings from any given incident or just the ones used in court? How will the recordings be stored? On a disc, on the prosecutors' server or in the cloud? Will storage be shared with the public defender (in jurisdictions where funding is the same source)? For how long will the recordings be retained if state statute does not govern retention of evidence? How can we avoid redundant storage costs between the entities in the criminal justice system?

The Future: Gauging the overall impact BWC videos will have on the criminal justice system is inherently difficult, and the impact of BWC recordings in court remains to be seen. A video with strong prosecutorial evidence may lead to a plea by the defendant, but many other factors may also play a role in the defendant's decision. A video that reflects poorly on a victim, witness, or officer may influence the decision of whether or not to file charges after video review. To quantify these outcomes would require possible disclosure of attorney-client communication or work product. Finally, juror evidentiary expectations will have to be managed, just as they were with the advent of DNA evidence.

One point is readily apparent: BWC evidence requires enhanced law enforcement and prosecution collaboration. In order for BWC videos to achieve effective outcomes, prosecutors must understand police field work well enough to know what will and will not be caught on video, and officers must help educate their courtroom partners about why certain enforcement actions unfold as they do. Conversely, prosecutors can point out to officers which recording practices help in court. Such mutual teaching and partnership can lead to improved evidence capture on BWCs that will lead to more effective courtroom presentations.

Suggestions for Consideration:

Develop standard training for law enforcement and prosecutors to:

Improve marking of videos to facilitate timely evidence review for charging

Improve/standardize labeling of videos to prevent loss of video evidence

Highlight best taping and court use practices to improve court outcomes; and

Create standards for storage responsibilities and costs to prevent duplicate expenditures and ensure required retention of evidence.

Richard W. Vorder Bruegge

Senior Physical Scientist, Federal Bureau of Investigation

Richard W. Vorder Bruegge is a Senior Physical Scientist in the Operational Technology Division of the Federal Bureau of Investigation where he is responsible for overseeing science and technology developments in the imaging sciences, as well as consulting on other more general science and technology issues across the FBI. He has worked at the FBI since 1995.

He has a Ph.D. and Master's degree in Geological Sciences from Brown University, as well as a Bachelor of Sciences in Engineering from Brown.

Dr. Vorder Bruegge is a fellow of the American Academy of Forensic Sciences, and in 2010 he was named a Director of National Intelligence Science and Technology Fellow for his work in facial recognition and identification. He is the Chair of the Digital & Multimedia Scientific Area Committee in the Organization of Scientific Area Committees for Forensic Science and so serves as a member of the Forensic Science Standards Board.

Department of Justice

SUPPORTING DOCUMENT

DR. RICHARD W. VORDER BRUEGGE
SENIOR SCIENTIST
OPERATIONAL TECHNOLOGY DIVISION OF THE
FEDERAL BUREAU OF INVESTIGATION

FOR THE

PRESIDENT'S COMMISSION ON
LAW ENFORCEMENT AND THE ADMINISTRATION OF JUSTICE

ON THE TOPIC OF

OPPORTUNITIES AND CHALLENGES POSED BY THE USE OF FACIAL RECOGNITION IN ADDRESSING VIOLENT CRIME

PRESENTED
APRIL 21, 2020

SUPPORTING DOCUMENT

DR. RICHARD W. VORDER BRUEGGE
SENIOR SCIENTIST
OPERATIONAL TECHNOLOGY DIVISION OF THE
FEDERAL BUREAU OF INVESTIGATION

FOR THE
PRESIDENT'S COMMISSION ON
LAW ENFORCEMENT AND THE ADMINISTRATION OF JUSTICE

ON THE TOPIC OF
OPPORTUNITIES AND CHALLENGES POSED BY
THE USE OF FACIAL RECOGNITION
IN ADDRESSING VIOLENT CRIME

PRESENTED
APRIL 21, 2020

Introduction

Law enforcement (LE) uses Facial[1] Recognition Technology (FRT) every day to help identify criminal suspects and deceased individuals, locate missing and exploited children, ensure that the right person is being released from custody, and more efficiently process seized evidence. This is done by individuals and agencies who take seriously their responsibilities to protect the privacy and civil liberties of suspects, victims and the rest of society.

Evolution of Facial Recognition Technology

The evolution of FRT began within LE in the late 1800s, when French criminologist Alphonse Bertillon developed a method of identification based on measurements of body dimensions (anthropometrics). This method was used by LE to help identify repeat convicted criminals. The dimension sets Bertillon used included measurements of the head and face, representing the first use of "face recognition" by LE. Bertillon's system was replaced in approximately 1915 by fingerprints which were much more reliable.

In the second half of the 20th century, researchers began developing computer-based approaches to facial matching. By the early 1990s, interest was high enough to lead the United States (U.S.) government to establish testing of algorithms. These tests ultimately became today's Face Recognition Vendor Tests (FRVT), now administered by the National Institute of Standards and Technology (NIST). Early testing in the mid-1990s demonstrated that advanced analysis of facial measurements—kind of a high-tech Bertillon system—did not work well in an automated system. When presented with the same person's face in two different images, these measurements failed to verify a person's identity 80 percent of the time (i.e., 80 percent error rate)[2]. This led

[1] This document makes no distinction between the terms "Facial Recognition" and "Face Recognition."

[2] Great care must be taken when discussing "error rates." The "false non-match" (or "miss") rates provided in this section (i.e., instances when a true match pair is not called a "match") are based on the following automated "verification" process: (1) Two face images are compared to generate a similarity score; (2) The system then makes a decision by comparing that similarity score to a user-defined threshold score, with three possible outcomes: (a) a correct verification ("true match"); (b) an incorrect verification (a "false match"); or (c) a false rejection ("false non-match"). How the user defines the threshold score will impact all three metrics (e.g., raising the threshold score can reduce the number of false matches, but it will probably increase the number of false non-matches, too). A more detailed description of error rates is beyond the scope of this paper.

serious FRT researchers (including commercial developers) to abandon anthropometry (measurements) and focus on "pattern matching" approaches.

A person's facial features create a unique "pattern." Much like a quilt, each feature contributes to the pattern. Mouth shape, nose positioning, eye and eyebrow shape, overall facial contours, and even skin texture make up the pattern. In "pattern matching" approaches, the algorithm creates a numerical representation of the facial pattern.[3] By 2013, pattern-matching approaches had achieved error rates below half of one percent (.5 percent) when comparing two mug-shot quality photographs of the same person (one-to-one).

However, the facial pattern recorded in an image can appear different from image to image due to a number of factors, including differences in illumination (e.g., darker or brighter), expression (e.g., neutral vs. smiling), subject pose (e.g., looking straight at the camera or at an angle), or aging. Recent advances in computer vision and machine learning (aspects of computer science related to artificial intelligence) have now made it possible to achieve error rates under one percent for faces in photographs with these challenges.

While individual algorithms vary in their details, the main reason that today's machine learning approaches work so well begins with the fact that they incorporate many photographs of each subject in their training. As a result, the algorithms are exposed to the changes in a subject's face under these different conditions, and by looking for common configurations across multiple subjects under different conditions, they are better able to predict how a given individual will appear under those conditions. Put another way, whereas "pattern matching" techniques of a decade ago may have relied upon comparison of individual features on the face, today's techniques rely upon the interrelationship of multiple features across the entire face under a variety of conditions.

How Does Law Enforcement Use FRT?

LE uses FRT in a variety of ways. FRT is used to help verify the identity of inmates before they are released, or to make the forensic examination of seized evidence more efficient by grouping together similar faces found on a suspect's device. Examples include locating potential victims of child exploitation on a suspected pedophile's computer or locating potential co-conspirators in a criminal organization if their photos are on the suspect's mobile phone. In the latter use case, an investigator would not know the identities of anyone in the photos, unless they were personally familiar with them, and only through subsequent investigative efforts would LE come to know their identities.

Investigators could try to identify an unknown person in the use case above by asking the suspect or his/her associates to identify the people in the photos, or they could use FRT to perform a "one-to-many search," which is the most well-known LE use of FRT.

How Should a One-to-Many FRT Search be Performed?

Most LE uses of FRT involve searching an image (the "probe") against a database of known subjects (the "gallery"). In these one-to-many searches (probe-to-gallery), best practice begins with a trained user. This user submits the probe to the system and the probe is converted to a template. This template is compared against the templates of every other face in the gallery. The highest matching gallery images are presented as a set of "returns" to the trained user in rank order. The highest scoring match is presented first, then the second highest score, etc. Different FRT systems allow the user to see up to 50 returns. This set of returns is referred to as the "candidate list." The user then examines the candidates to determine if any of them represents a viable investigative lead.

The user should check each face in the candidate list for a potential match to the probe. Morphological analysis is the recommended technique used to compare individual features of the faces in the probe and gallery images.

[3] The numerical representation is referred to as the "template."

Through morphological analysis, the user may quickly eliminate some candidates as potential matches through gross features, such as overall size and shape of the head, face, or nose; separation of the eyes; or the degree the ears protrude from the head. If a candidate cannot be eliminated based on gross features, more detailed features are considered, such as the shape of the eyes, nose, mouth, and ears; creases on the forehead and cheeks; and freckles, moles, and scars. These details allow a user to eliminate most, if not all, of the candidates in the returned set.

If a candidate cannot be eliminated based on observed differences, the user may determine the candidate is a valid investigative lead. This does not mean that the candidate has been "positively identified" as the subject in the probe image. It only indicates that the user of the FRT system has determined the candidate is worth further investigation as potentially being that subject.

In many LE applications, once a user identifies a potential candidate, a second trained user verifies the results as valid. If the second user disagrees with the finding, a third user (perhaps a supervisor) is required to "break the tie." If the third user agrees with the first user's determination, the originator of the request will be informed that a valid investigative lead has been found.

More times than not – as with other investigative techniques - no investigative lead is generated through a one-to-many search, and investigators must identify a suspect in some other way. Last year, former New York Police Commissioner James O'Neill described in a New York Times OpEd how, in 2018, NYPD conducted over 7,000 FRT searches, resulting in over 1800 investigative leads. These number reflect other agencies reporting, as well, and highlight a key aspect of LE's use of FRT: Every facial recognition search conducted by LE today does not result in the identification of a suspect for further investigation. Rather, trained LE officials review a candidate list and determine if any subject is worth investigating further.

Candidates developed as investigative leads through FRT should never be described as "positive identifications." In fact, the U.S. Department of Justice Bureau of Justice Assistance's (DOJ-BJA) Face Recognition Policy Development Template recommends the following wording:

"The [name of entity] is providing this information as a result of a search, utilizing face recognition software, of records maintained by the [name of records entity]. This information is provided only as an investigative lead and IS NOT TO BE CONSIDERED A POSITIVE IDENTIFICATION OF ANY SUBJECT. Any possible connection or involvement of any subject to the investigation must be determined through further investigation and investigative resources."

RECOMMENDATION # 1 – Human review is a crucial piece of LE's use of FRT. Therefore, it is critical that those reviewers be trained in how to perform this task. LE should require standardized training for any official who would use face recognition technology. The FBI and other agencies have developed such training which meets standards set by the Facial Identification Scientific Working Group (FISWG)[4], but more resources are be needed to make it available for delivery in person or online for those who need it.

RECOMMENDATION # 2 – Testing has shown that that the professionals who adjudicate those candidate lists are very good at it[5]. However, we need to develop a mechanism to deliver similar tests and training on a regular basis to ensure that the people who perform this job maintain their proficiency from year to year. The government should support the further development and implementation of proficiency tests and recurring training for LE professionals conducting FRT adjudications.

Where do Probe and Gallery Photographs Used by LE come from?

[4] See FISWG documents which are included in the sources of additional information.
[5] See article by Phillips et al., 2018, which is included in the sources of additional information.

LE officers submit probe photos that may be collected in the course of their investigations for search against available galleries. Examples of probe photos (the "one" in "one-to-many") include the following: a bank robbery surveillance image; a social media photo shared by a suspect with an undercover officer or shared by a victim; and a mug shot or passport photo used to locate a known fugitive entered in a public database under an alias. Other probe examples include: a photograph taken by an LE officer of a deceased or unconscious accident victim; and a photograph taken by an LE officer of a lawfully detained subject who is unable or unwilling to provide valid identity documents. The latter two examples reflect the predominant type of mobile face recognition used in the United States.

Galleries maintained by LE agencies consist, for the most part, of criminal mug shot photographs. Some state's LE agencies may also maintain galleries which include driver license photos. They do not contain random photographs of people taken in public places.

In addition to such LE-managed galleries, LE often has access to other galleries, including driver license galleries, other government repositories, and missing person databases. Recently, some commercial services have come online which offer facial recognition searches to customers using databases of images they have collected from other sources, including social media sites. Such services may be helpful in locating individuals whose pictures would not otherwise be found in mug shot, driver license, or missing person databases.

Need for Documented Policies

In the United States criminal justice agencies have a duty to examine the privacy, civil rights, and civil liberty implications of their information systems and sharing practices, and to implement policies that will protect the rights of individuals who are either suspected of, or victimized by, crime. Many agencies choose to publish their findings in the form of a Privacy Impact Assessment (PIA). For face recognition systems, agencies need to establish clear policies regarding how the systems will be used. The U.S. DOJ-BJA has published guidance on preparing PIAs and has also published guidance for law enforcement agencies interested in developing face recognition policies. Both documents are appended to this statement as sources of additional information.

RECOMMENDATION # 3 –Law enforcement agencies should establish written policies for how they plan to implement facial recognition, including the source of images contained in their galleries. A further aspect of this recommendation is that agencies should implement governance policies and auditing to ensure they are following their documented procedures. This recommendation also applies to any use of commercial face recognition services.

Additional Challenges and Opportunities

Over the last 30 years, the performance of FRT algorithms has improved dramatically. In a one-to-many search, today's best algorithms can return a subject as the top scoring candidate 99 percent of the time, as long as the subject is in the gallery. This holds true for individuals across different demographic groups, including groups of ancestry, age, and sex.

All algorithms are not the same, however, and many algorithms tested by the NIST in 2019[6] show performance differences for subjects in various demographic groups. However, a number of these algorithms, including several used by federal and other government agencies, did not show any measurable differentials when tested under the one-to-many search conditions described above. This highlights the fact that not all FRT algorithms are the same. LE agencies have a responsibility to be aware of any limitations of their specific algorithms and

[6] This NIST evaluation (available at: https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf) tested 189 different algorithms from 99 developers, and included well-developed commercial algorithms, as well as brand new algorithms in their first stage of development.

systems and take steps to mitigate such limitations, if necessary. FISWG has provided guidance on practices that FRT system administrators and users can implement to increase overall performance[7].

Fortunately, standard practice within LE for one-to-many FRT searches provides the most significant mitigation possible: human adjudication of the candidate list by trained professionals. No LE agency should rely solely on the highest scoring output of an FRT one-to-many search to determine if a valid investigative lead is present.

RECOMMENDATION # 4 – LE agencies should implement regular testing of their FRT systems to ensure that the performance meets or exceeds expectations, and take appropriate steps to ameliorate any deficiencies, including regular upgrades of the underlying algorithm.

Finally, the United States is fortunate to have the NIST infrastructure in place to constantly perform tests of FRT algorithms. Their efforts over the last 30 years have pushed industry and academia to constantly improve the accuracy of this technology. Although FRT is now helping LE on a daily basis, there is still room for improvement. As noted above, some algorithms display differential performance for different demographic groups. Likewise, accuracy challenges remain when dealing with images depicting children or challenging conditions such as poor resolution or harsh lighting. Academic and commercial developers of FRT algorithms should be encouraged to improve their algorithms to meet those challenges.

RECOMMENDATION # 5 – LE agencies and the Federal Government should continue to support NIST testing of FRT algorithms under a variety of conditions to ensure that these algorithms can meet the needs of the LE user community.

In closing, FRT is a tool that works for LE. It can be – and is – used in a way that protects the public's privacy and civil liberties.

[7] See FISWG Facial Recognition Systems: Methods and Techniques in the sources of additional information.

SOURCES OF ADDITIONAL INFORMATION

1. US DOJ Bureau of Justice Assistance **Facial recognition policy development template**: https://bja.ojp.gov/sites/g/files/xyckuh186/files/Publications/Face-Recognition-Policy-Development-Template-508-compliant.pdf
2. US DOJ Bureau of Justice Assistance **Guide to Conducting Privacy Impact Assessments** https://it.ojp.gov/documents/d/Guide%20to%20Conducting%20Privacy%20Impact%20Assessments_compliant.pdf
3. FISWG **Guide for Facial Comparison Training of Reviewers to Competency** https://fiswg.org/draft_fiswg_guide_comparison_training_reviewers_v1.0_20191025.pdf
4. FISWG **Minimum Training Criteria for Assessors Using Facial Recognition Systems** https://fiswg.org/draft_fiswg_guide_comparison_training_assessors_using_frs_v1.0_20191025.pdf
5. FISWG **Facial Recognition Systems: Methods and Techniques** https://fiswg.org/FISWG_fr_systems_meth_tech_v1.0_2013_08_13.pdf
6. Phillips et al., **Face recognition accuracy of forensic examiners, superrecognizers, and face recognition algorithms**, PNAS June 12, 2018 115 (24) 6171-6176; first published May 29, 2018 https://doi.org/10.1073/pnas.1721355115
7. National Sheriffs' Association Case Examples (attached)
8. **IJIS-IACP Facial Recognition Use Case Catalogue** https://cdn.ymaws.com/www.ijis.org/resource/collection/93F7DF36-8973-4B78-A190-0E786D87F74F/Law_Enforcement_Facial_Recognition_Use_Case_Catalog.pdf
9. **Joint letter to Congress led by Information Technology and Innovation Foundation**: https://itif.org/publications/2019/09/26/open-letter-congress-facial-recognition
10. **Center for Data Innovation public survey on LE use of facial recognition** https://www.datainnovation.org/2019/01/survey-few-americans-want-government-to-limit-use-of-facial-recognition-technology-particularly-for-public-safety-or-airport-screening/

Bureau of Justice Assistance
U.S. Department of Justice

Face Recognition

Policy Development Template

For Use in Criminal Intelligence and Investigative Activities

December 2017

Where to Locate This Resource

This resource is available at www.it.ojp.gov and www.ncirc.gov. To request printed copies, send requests to information@ncirc.gov.

To Request a Word Version of the Template

To request a Word version, send requests to information@ncirc.gov.

Updates

This resource is considered a living document. Submission of feedback and content suggestions for periodic updates are encouraged and may be provided by e-mail to information@ncirc.gov.

This project was supported by Grant Number 2013-D6-BX-K001 awarded by the Bureau of Justice Assistance, in collaboration with the U.S. Department of Homeland Security. The Bureau of Justice Assistance is a component of the Department of Justice's Office of Justice Programs, which also includes the Bureau of Justice Statistics, the National Institute of Justice, the Office of Juvenile Justice and Delinquency Prevention, the Office for Victims of Crime, and the Office of Sex Offender Sentencing, Monitoring, Apprehending, Registering, and Tracking. Points of view or opinions in this document are those of the author and do not necessarily represent the official position or policies of the U.S. Department of Justice or the U.S. Department of Homeland Security.

Face Recognition Policy Template for State, Local, and Tribal Criminal Intelligence and Investigative Activities

(This Page Intentionally Left Blank)

Table of Contents

I. Introduction

Face recognition technology can be a valuable investigative tool to detect and prevent criminal activity; reduce an imminent threat to health or safety; protect the public; help identify persons unable to identify themselves, or deceased persons; and improve security and officer safety. The National Center for Missing and Exploited Children (NCMEC), for example, is using face recognition software to search the internet for these children. In the past, determining someone's identity was a manual drawn-out process of viewing mug shot images. The use of face recognition software is helping to streamline this process by returning investigative results quicker. The purpose of face recognition technology is not a new one, it's simply enabling law enforcement entities to complete an existing process more efficiently.

However, law enforcement's use of face recognition tools in investigative and criminal intelligence activities has been the subject of much scrutiny regarding concerns about the accuracy of the technology, use at First Amendment-protected events, and assertions that face recognition systems are being used without appropriate safeguards, such as law, policy, training, and audits. Since images of individual persons are the source of face recognition information, there are higher expectations for the protection of privacy, civil rights, and civil liberties (P/CRCL). Currently, there is no uniform set of rules in the United States governing the gathering, collection, use, sharing, and dissemination of information available through face recognition tools. The potential for misuse of face recognition information may expose agencies participating in such systems to civil liability and negative public perceptions. The lack of rules and protocols also raises concerns that law enforcement agencies will use face recognition systems to systematically, and without human intervention, identify members of the public and monitor individuals' actions and movements. Strong control and oversight of face recognition use are critical considerations in policy development and program implementation. Such efforts not only enhance mission effectiveness but also safeguard P/CRCL of individuals.

This policy development template was developed by state, local, and federal law enforcement, privacy, and criminal justice partners to provide law enforcement, fusion centers, and other public safety agencies with a framework for developing face recognition policies that comply with applicable laws, reduce privacy risks, implement minimum required training for authorized users and examiners, and establish entity accountability and oversight. In addition, this template includes policy provisions on collection, access, use, dissemination, data quality, security, redress, retention and purging, and accountability and enforcement, with an overall focus on ensuring the integration of P/CRCL protections in face recognition processes. Established Fair Information

Practice Principles form the core of the privacy framework for this template (see Appendix B). Note: The term "entity" is used throughout this resource to refer to the policy-authoring organization.[1]

When an entity determines to develop and implement a face recognition policy, it is important to note that crafting such a policy is not a one-time project; it is just one stage in an ongoing entity privacy program cycle:[2]

Stage 1. Educate and raise awareness on the importance of having P/CRCL protections.
Stage 2. Assess entity P/CRCL risks by evaluating the process through which the entity collects, receives, accesses, uses, disseminates, retains, and purges face recognition information.
Stage 3. **Develop a face recognition policy** to articulate the legal framework and policy position on how the entity handles face recognition.
Stage 4. Perform a policy evaluation and engage with community stakeholders, prior to publishing, to determine whether the policy adequately addresses current standards, P/CRCL protections, and the law.
Stage 5. Implement and train personnel and authorized users on the established rules and procedures.
Stage 6. Perform an annual policy review and make appropriate changes in response to implementation experience, guidance from oversight or advisory bodies, applicable laws, technology, and public expectations.
Stage 7. Audit the processes described in the face recognition policy.

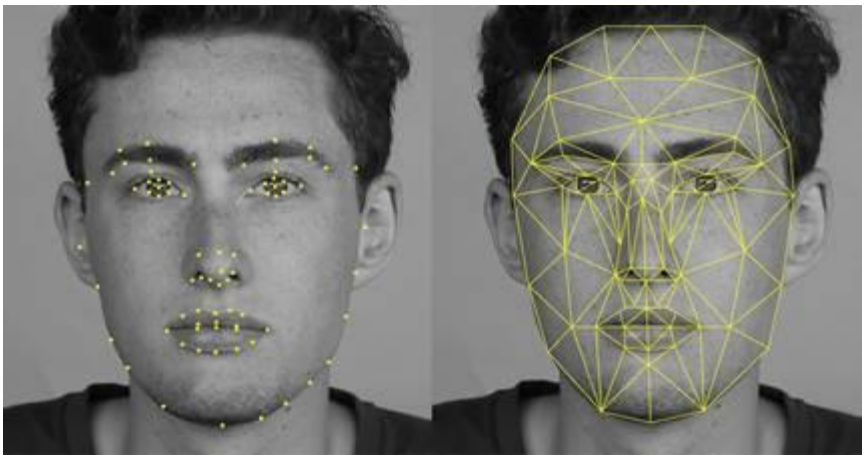
The implementation of proven policies and practices can mitigate the risk of negative impacts while improving mission effectiveness. As face recognition use expands, it is necessary for law enforcement, fusion centers, and other public safety agencies to ensure that comprehensive policies are developed, adopted, and implemented in order to guide the entity and its personnel in the day-to-day access and use of face recognition technology. Policies that are developed in a transparent manner and which are properly enforced foster trust—not only within and between justice partners but also by the public. This process helps ensure that justice entities are serving as responsible stewards of face recognition information and operating with respect for individual P/CRCL and the law.

BIOMETRICS POLICIES

This template was developed to address the use of face recognition technology by state, local, tribal, and territorial (SLTT) law enforcement and public safety entities and fusion centers through the development of P/CRCL policies. It was not, however, designed to cover all possible biometric modalities, such as fingerprints, palm prints, DNA, familial DNA searching, iris recognition, retina scan, voiceprint, etc. Specific and comprehensive policies are recommended that will appropriately address the use of each biometric technology, unique capture methods, complex processes and procedures, and P/CRCL protections.

[1] The term "entity" is used throughout this resource to identify the policy-authoring organization and differentiate it from external or participating agencies. Refer to the terms "agency," "entity," and "participating agency" in Appendix A—Glossary of Terms and Definitions for more information.
[2] Global Justice Information Sharing Initiative Privacy Resources, Bureau of Justice Assistance, Office of Justice Program, U.S. Department of Justice, https://it.ojp.gov/privacy.

A. Face Recognition Overview



Considering the potential benefits to public safety that face recognition technology can offer, it is important that law enforcement and public safety agencies establish the appropriate framework for ensuring that the technology will be used in a responsible manner that does not violate P/CRCL.

Use of face recognition technology is often misunderstood. It is not being used as an all-knowing big brother that keeps track of an individual's weekly—or daily—trips to a business. More accurately, it is a lead generator for law enforcement to investigate criminal activity, akin to a more reliable eye witness. Moreover, facial recognition is not a machine-dominated technology. Generally, entities use—and it is a good practice to do so—a two-part machine-human process—facial recognition, which is software based, and facial comparison, which is human based.[3]

1. How Do Face Recognition Systems Work?

During enrollment, an image (e.g., a photograph, a digital capture, or a video still) of a face of the known individual (such as a mug shot) is submitted to the face recognition system. While each system's techniques may vary, in general, the distinctive characteristics of each face, such as the distance between the eyes, the width of the nose, and the depth of the eye sockets, are measured. These characteristics are known as "nodal points." Nodal points are extracted from the face image and are transformed through the use of algorithms into a unique file called a "biometric template."[4] A biometric template is a reduced set of data that, in face recognition systems, represents the unique features of the enrolled person's face.

Biometric templates are then stored in a repository for future comparison with probe images of unknown persons, such as images gathered during a criminal investigation. During a face recognition search, the system compares the biometric template created from a probe (unknown) image with all of the face templates (of known persons) stored in the repository. The system then provides a list of the most likely candidate photographs (sometimes referred to as a "gallery"[5]). At this point in the process, the face recognition system has not made a formal identification.

Algorithms

Algorithms are mathematical equations—calculations, data processing, or automated reasoning—that are widely used throughout information technology and are the biggest factors in face recognition accuracy. Since the development of, and improvements in, algorithm performance are ongoing and ever evolving, they are not discussed in depth within this resource. However, policy provisions on data quality are provided in section H. Data Quality in the P/CRCL template contained in Chapter II. Entities are strongly encouraged to consider algorithm performance prior to purchasing a face recognition system.

Refer to the National Institute of Standards and Technology's (NIST's) Face Recognition Vendor Tests (FRVT), which provide independent government evaluations of commercially available and prototype face recognition technologies, https://www.nist.gov/programs-projects/face-recognition-vendor-test-frvt.

[3] Ibid.

[4] The term "template," in this usage (e.g., biometric template), is not to be confused with the term used in the title of this document, which means a template, or guide, for developing a face recognition policy. To avoid confusion, the term biometric template is not used in the rest of this document but is used here for informational purposes only.

[5] The term "gallery" is sometimes used by entities when referring to the resulting candidate list. For the purposes of this document, the phrase "list of most likely candidates" will be used.

After the list is generated, trained human examiners follow-up on the list of most likely candidates by performing analysis to compare the probe photograph with the candidate photographs.

While **face recognition** is an automated computer evaluation of similarities between face images, **face comparison** is a manual examination of the differences and similarities between two face images or a live subject and a face image (one-to-one) for the purpose of determining whether they represent the same or different persons. The process is used in concert with standard investigative techniques.

2. Are Face Recognition Results Considered an Identification?

Face recognition search results are not considered positive identification and do not establish probable cause, without further investigation; rather, they are advisory in nature as an investigative lead only. Any possible connection or involvement of an individual to a criminal investigation must be determined through further analysis and investigation.

3. Is Face Recognition Information Considered Criminal Intelligence?

The policy template in Chapter II was developed to articulate entity policies and P/CRCL protections for the collection, receipt, access, use, dissemination, retention, and purging of face recognition information that is ***not yet*** part of a criminal intelligence or investigative file. If, after completing the analytic process, face recognition information is downloaded into a criminal intelligence or investigative file, the information is then considered criminal intelligence or investigative information and the laws, regulations, and policies applicable to that type of information govern its use.[6]

Law enforcement, fusion centers, criminal intelligence units, and other public safety entities utilize different types of information, such as criminal history, suspicious activity reports (SARs), and criminal intelligence as part of their criminal intelligence or investigative activities. Each type is governed by laws, regulations, and policies to authorize and ensure appropriate collection, receipt, access, use, dissemination, retention, and purging. Face recognition information—probe photographs, image repositories, lists of most likely candidates, etc.—is not considered criminal intelligence,[7] criminal history, or SAR information. As such, the laws, regulations, and policies that specifically apply to those types of situations may not apply to face recognition information ***until*** such time as it is downloaded and incorporated into a criminal intelligence or investigative case file. It is the further analytic and investigative processes by trained examiners that associate face recognition results with an identifiable individual.

B. How to Use This Resource

This resource contains a P/CRCL policy template in Chapter II. The provisions suggested in the template can be incorporated into the entity's general operational policies and day-to-day operations which must provide explicit and detailed P/CRCL protection guidance to entity personnel and other authorized sources

[6] This does not mean that face recognition information is not accorded protections until it is incorporated into a criminal intelligence or investigative file; rather, the provisions of this template were designed to articulate such protections. For example, use and dissemination of face recognition is addressed in Chapter II, Section F. Use of Face Recognition Information, and Section G. Sharing and Disseminating Face Recognition Information.

[7] The operating principles of 28 CFR Part 23 provide guidance to law enforcement regarding how to effectively operate criminal intelligence information systems while safeguarding P/CRCL. The regulation applies, as a matter of law, to state, local, tribal, or territorial agencies if they are operating interjurisdictional or multijurisdictional criminal intelligence systems that are supported with Omnibus Crime Control and Safe Streets Act funding. See 28 CFR Part § 23.3. For participating or member agencies, the intelligence project's operating policies, as set forth in a participation or membership agreement, govern their submission, access, use, retention/destruction, and any third-party dissemination of criminal intelligence information received from the intelligence project. For further information, see https://28cfr.iir.com/Resources/Executive-Order. Those entities that are not subject to 28 CFR Part 23 may voluntarily adopt the protections articulated in 28 CFR Part 23 as a matter of policy.

and participating agencies. Each section of the template is a fundamental component of an overall comprehensive face recognition policy.

The template in Chapter II groups policy concepts together (e.g., governance, accountability, security, etc.) into categories, with each category containing policy provisions that relate to that category. Policy provisions are presented as questions to the policy drafter and the drafter then answers by writing policy language, working through each question to build a complete policy. Policy questions and guidance and best practices are shown in **bold type**. To assist policy authors in drafting a policy, sample policy language is provided below each bolded question in regular type, as follows:

> 1. **A bolded policy question that the entity will answer with written policy provisions.**
>
> **Notes and best practices are also shown under each question in bold.**
> **[Special instructions, if any, are bolded and bracketed under each question.]**
>
> Sample policy language is provided underneath each policy question in plain text. If used, this language MUST be customized by filling in the bracketed items, such as the **[name of the entity]**.

In addition, throughout the template, several terms are **underlined and hyperlinked** to their definitions in Appendix A. Glossary of Terms and Definitions, to assist policy drafters in understanding the terminology used.

1. Program Versus System

To aid in the reader's understanding, the following describes this resource's use of the terms "face recognition program" and "face recognition system."

- **Face Recognition Program**—A term used in this resource to describe an entity's face recognition initiative, which includes the management of human components (management, analysts, examiners, authorized users), ownership and management of the face recognition system (technical components, see below), and the establishment and enforcement of entity-wide processes, policies, and procedures.
- **Face Recognition System—**A term used in this resource to describe the technical components of a face recognition program, such as hardware, software, interfaces, image repositories, templates, autogenerated candidate lists, etc. While some entities own such a system (see above), others may have authorized access to another entity's face recognition system.

2. What Entities Should Use the Policy Template?

The policy template, contained in Chapter II, is designed for use by state, local, tribal, and territorial (SLTT) law enforcement entities, fusion centers, and other public safety agencies that either own and operate their own face recognition program or only have direct access to, and authorized use of, another entity's face recognition system. Entities are guided to adopt and customize the provisions of the template that apply to the entity's face recognition system or program.

An entity must set forth in a formalized agreement, such as a memorandum of understanding (MOU) or interagency agreement, the essential requirements for submitting face recognition search requests by external agencies to the entity. The policy provisions in Chapter II's template may be useful to inform the key components of the formalized agreement. For example, the entity may require requesting agencies to complete specialized training, as referenced in Chapter II, Section N. Training, item 4.

3. Transparency and Referencing Other Policies

Frequently, agencies already have established privacy-related policies and procedures that may be contained in broader policy documents (e.g., concept of operations, standard operating procedures, user agreements, and employee handbooks). There may also be cross over between the provisions in this template and other policies, such as an entity's social media or general privacy policy. In accordance with Chapter II, Section M. Accountability and Enforcement, and Subsection M.1. Transparency, agencies are strongly encouraged to make their face recognition policies available to the public, even if the other existing policies or procedures are not made publicly available.

Agencies are cautioned against providing cross-references within their face recognition policies to policy provisions contained in other policies that are not available to the public, without excerpting the relevant text. Providing a cross-reference to, for example, a numbered section (e.g., "policy number 201.56-B, section 6.a.") within a non-publicly available policy, without excerpting the relevant text will confuse the reader (e.g., if the reader is not an employee and does not have access to policy 201.56-B). As such, the reader will not know what is meant by the numeric cross-reference. For this reason, it is better to excerpt (or restate) the actual language of the specific policy provision the entity wants to emphasize within the face recognition policy. As a best practice, only cross reference policies that are publicly available or restate (excerpt) the applicable language within the face recognition policy.

> **CAUTION**
>
> Do not assume that an existing policy (for example, on fingerprints) will automatically apply to other biometric technologies without a thorough assessment of similarities and differences of biometrics, regulations, etc.

4. Mobile Face Recognition Use

Mobile face recognition applications generally use an image of an individual, which is captured in the presence of a law enforcement officer in the field. Then, using a mobile interface, the image is submitted as a probe photograph to search image repositories, which can result in a list of most likely candidate images. Trained law enforcement officers evaluate the candidate images using standard investigative techniques to make a determination of whether the person in front of them is an individual shown in the candidate result listing.

Law enforcement use of mobile face recognition devices and applications is an area where public concern has been raised. This resource does not take an official position on mobile use of this technology. However, it is highly recommended that if an entity makes a decision to implement and utilize mobile face recognition applications, it should do so **only** after vetting the decision, requiring appropriate training for officers who are authorized to capture remote face images and use mobile search applications, and developing comprehensive policies to address such use. To assist entities in policy development to specifically address mobile use of this technology, the following provisions were added to the policy template and are contained in Chapter II of this resource.

- Section A, Purpose Statement, provision number 3
- Section F, Use of Face Recognition Information, provision number 6
- Section F, Use of Face Recognition Information, provision number 7
- Section F, Use of Face Recognition Information, provision number 8
- Section N, Training, provision number 5

Additional face capture training and other provisions may also be needed, depending on the entity's unique use of this technology in the field. If the entity does not utilize mobile face recognition, these provisions will not apply when the entity is developing a non-mobile face recognition policy. Another option is for the entity to add policy provisions that specifically articulate the entity's exclusion of mobile face recognition use. Either choice is acceptable. What is important is the entity develop a face recognition policy that accurately describes its operations and compliance with applicable laws, regulations, policies, rules, or other constraints in all uses of the technology.

5. Face Recognition Analysis on Live Video

Face recognition analysis on live video is different than mobile face recognition. While mobile face recognition entails using a mobile device to capture a photo of a subject who is in the presence of a law enforcement officer, such as during a traffic stop, face recognition analysis on live video means that face recognition searches may be performed on images of any individual captured within the frame of a live feed video camera (such as a closed circuit television).

It is important for the entity to articulate a clear and affirmative statement regarding the entity's position regarding face recognition analysis on live video. To assist entities during policy development, provision F. Use of Face Recognition Information, item 3., was added to the policy template, in Chapter II of this resource, to specifically address face recognition analysis on live video.

6. Template Modifications—Customizing Your Policy

It is important to note that the policy development template in Chapter II **is not intended to be used as is** without modification. Nor is it intended to create inconsistencies with applicable laws and regulations. The sections represent the suggested foundational components of an effective face recognition policy but do not cover all situations, processes and procedures, or the applicable constitutional provisions, laws, ordinances, or regulations that may be unique within your state. The template represents a starting point for your entity to establish baseline face recognition policy guidelines. Law enforcement and public safety entities are encouraged to complete as many of the template questions as are applicable; to enhance sections to include items such as references to applicable statutes, rules, standards, or policies; and to add sections for provisions that are not addressed in the template.

To facilitate this process, the following appendices have been developed for review and customization, as appropriate, and should be referenced in each entity's face recognition policy:

- Appendix A—Glossary of Terms and Definitions
- Appendix B—Fair Information Practice Principles (FIPPs)
- Appendix C—Listing of Federal Laws

It is important that entities review each of the policy questions, as well as the notes, references, and instructional information provided with each, when drafting entity policy language. However, to assist entities in the drafting and customization process, all of the sample policy language contained in the template has been extracted and provided in Appendix D, Sample Face Recognition Policy.

C. Resource List

The following list provides useful face recognition and biometric-related resources, policy development templates, privacy regulations and authorities, and other resources that may be of interest:

1. Face Recognition and Biometric-Related Resources

- ***Biometric Specifications for Personal Identity Verification***, NIST Special Publication 800-76-2, National Institute of Standards and Technology (NIST), U.S. Department of Commerce, July 2013, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-76-2.pdf.

- ***Capture and Equipment Assessment for Face Recognition Systems***, Version 1.0, Facial Identification Scientific Working Group (FISWG), May 5, 2011, https://www.fiswg.org/FISWG_CaptureAndEquipmentAssessmentForFRSystems_v1.0_2011_05_05.pdf.

- ***Data Format for the Interchange of Fingerprint, Facial, and Other Biometric Information***, 2011 American National Standard for Information Systems, Information Technology Laboratory (ITL),

American National Standards Institute/National Institute of Standards and Technology (ANSI/NIST), Update 2015, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.500-290e3.pdf.

- ***Electronic Biometric Transmission Specification*** (EBTS), NGI-DOC-01862-x.x., Criminal Justice Information Services (CJIS), Federal Bureau of Investigation (FBI), www.fbibiospecs.cjis.gov.

- **Face Recognition Challenges and Evaluations** (FaCE), NIST, https://www.nist.gov/programs-projects/face-challenges.

- **Face Recognition Technology (FERET) Program**, Department of Defense (DoD) Counterdrug Technology Development Program Office, https://www.nist.gov/programs-projects/face-recognition-technology-feret.

- **Face Recognition Vendor Test (FRVT)**, NIST, https://www.nist.gov/programs-projects/face-recognition-vendor-test-frvt.

- **FRVT—Performance of Automated Gender Classification Algorithms**, NIST Interagency/Internal Report (NIST IR) – 8052, April 2015, https://www.nist.gov/publications/face-recognition-vendor-test-frvt-performance-automated-gender-classification.

- **FRVT—Performance of Face Identification Algorithms**, NIST IR 8009, May 21, 2014, https://www.nist.gov/publications/face-recognition-vendor-test-frvt-performance-automated-gender-classification.

- ***Facial Comparison Overview***, Version 1.0, FISWG, April 29, 2010, https://www.fiswg.org/FISWG_Facial_Comparison_Overview_v1.0_2010.04.29.pdf.

- **Facial Identification Scientific Working Group**, https://www.fiswg.org/.

- ***Facial Image Comparison Feature List for Morphological Analysis***, Version 1.0, FISWG, November 22, 2013, https://www.fiswg.org/FISWG_1to1_Checklist_v1.0_2013_11_22.pdf.

- ***Facial Recognition System: Methods and Techniques***, Version 1.0, FISWG, August 13, 2013, https://www.fiswg.org/FISWG_fr_systems_meth_tech_v1.0_2013_08_13.pdf.

- ***Facing Facts: Best Practices for Common Uses of Facial Recognition Technologies***, Federal Trade Commission, October 2012, https://www.ftc.gov/reports/facing-facts-best-practices-common-uses-facial-recognition-technologies.

- ***Glossary***, Version 1.1, FISWG, February 2, 2012, https://www.fiswg.org/FISWG_Glossary_v1.1_2012_02_02.pdf.

- ***Guidelines for Facial Comparison Methods***, Version 1.0, FISWG, February 2, 2012, https://www.fiswg.org/FISWG_GuidelinesforFacialComparisonMethods_v1.0_2012_02_02.pdf.

- ***Information Technology: American National Standard for Information Systems-Data Format for the Interchange of Fingerprint, Facial, & Other Biometric Information***, NIST Special Publication 500-290, November 2011, http://ws680.nist.gov/publication/get_pdf.cfm?pub_id=910136.

- ***Information Technology—Vocabulary—Part 37:Biometrics***, International Standard, International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), ISO/IEC 2382-37, Second edition, February 2017, http://standards.iso.org/ittf/PubliclyAvailableStandards/c066693_ISO_IEC_2382-37_2017.zip.

- ***Photograph Finish—Your Mug Shots Should Look Much Like This***, April 9, 2014, CJIS link, Criminal Justice Information Services (CJIS), Federal Bureau of Investigation (FBI), https://www.fbi.gov/services/cjis/cjis-link/photo-finish-your-mug-shots-should-look-much-like-this.

- ***Privacy and Information Quality Risks: Justice Agency Use of Biometrics***, Global Justice Information Sharing Initiative (Global), Bureau of Justice Assistance (BJA), Office of Justice Programs (OJP), U.S. Department of Justice (DOJ), September 1, 2011, http://it.ojp.gov/gist/77/Privacy-and-Information-Quality-Risks--Justice-Agency-Use-of-Biometrics.

- ***Privacy Best Practice Recommendations for Commercial Facial Recognition Use,*** National Telecommunications and Information Administration (NTIA), U.S. Department of Commerce, June 15, 2016, https://www.ntia.doc.gov/files/ntia/publications/privacy_best_practices_recommendations_for_commercial_use_of_facial_recogntion.pdf.

- ***Standards and Guidelines for Forensic Art and Facial Identification,*** International Association of Identification, April 2010, https://www.theiai.org/disciplines/art/ForensicArtGuidelinesSGFAFI1stEd.pdf.

- ***Video Evidence: A Law Enforcement Guide to Resources and Best Practices,*** Global, BJA, OJP, DOJ, March 2014, http://it.ojp.gov/gist/164/Video-Evidence--A-Law-Enforcement-Guide-to-Resources-and-Best-Practices.

2. Policy Development Templates

In addition to this resource, the following policy templates were developed through support of the Global Justice Information Sharing Initiative's Criminal Intelligence Coordinating Council, sponsored by the Bureau of Justice Assistance, Office of Justice Programs, U.S. Department of Justice, in collaboration with the U.S. Department of Homeland Security (DHS). Each is designed to assist justice entities in developing P/CRCL policies, including the use of social media and license plate readers in intelligence and investigative activities.

- ***Developing a Policy on the Use of Social Media in Intelligence and Investigative Activities: Guidance and Recommendations***, Global, BJA, OJP, DOJ, February 2013, https://it.ojp.gov/GIST/132/Developing-a-Policy-on-the-Use-of-Social-Media-in-Intelligence-and-Investigative-Activities--Guidance-and-Recommendations-.

- ***Fusion Center Privacy Policy Development: Privacy, Civil Rights, and Civil Liberties Policy Template***, DHS and DOJ, April 2010, https://it.ojp.gov/gist/48/Fusion-Center-Privacy-Policy-Development--Privacy--Civil-Rights--and-Civil-Liberties-Policy-Template.

- ***License Plate Reader Policy Development Template for Use in Intelligence and Investigative Activities***, Global, BJA, OJP, DOJ, February 2017, https://it.ojp.gov/GIST/1197/License-Plate-Reader-Policy-Development-Template-for-Use-in-Intelligence-and-Investigative-Activities.

3. Privacy Regulations and Authorities

Refer to Appendix C for synopses of primary federal laws that an entity should review and, where appropriate, consider citing in the face recognition policy to protect face recognition data and any personally identifiable information later associated with the face recognition information. As face recognition information may be incorporated as only one piece of information into a larger case file, the federal laws described in Appendix C may be applicable.

- Code of Federal Regulations (CFR), Title 28 (28 CFR)—Judicial Administration, Chapter 1—U.S. Department of Justice, Part 23—***Criminal Intelligence Systems Operating Policies***, http://it.ojp.gov/documents/28CFR_Part_23.pdf.

- ***Fair Information Practice Principles***, refer to Appendix B.

- ***Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule: A Guide for Law Enforcement***, U.S. Department of Health and Human Services (HHS), September 2013, https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/special/emergency/final_hipaa_guide_law_enforcement.pdf.

4. Additional Privacy and Security-Related Resources

- ***Criminal Justice Information Services (CJIS) Security Policy***, Version 5.5, CJISD-ITS-DOC-08140-5.5., June 1, 2016, CJIS, FBI, https://www.fbi.gov/services/cjis/cjis-security-policy-resource-center.

- **Federal Privacy Council**, https://www.fpc.gov/federal-privacy-council/.

- ***Guidelines to Ensure That the Information Privacy and Other Legal Rights of Americans Are Protected in the Development and Use of the Information Sharing Environment*** (ISE Privacy Guidelines), Office of the Program Manager, Information Sharing Environment (ISE), https://www.dni.gov/index.php/ic-legal-reference-book/guidelines-to-ensure-that-the-information-privacy-and-other-legal-rights-of-americans-are-protected-in-the-development-and-use-of-the-information-sharing-environment.

- **Office of Privacy and Civil Liberties, U.S. Department of Justice,** https://www.justice.gov/opcl.

- ***Preparing for and Responding to a Breach of Personally Identifiable Information***, Office Management and Budget (OMB) Memorandum M-17-12, (January 13, 2017), https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2017/m-17-12_0.pdf.

- ***Privacy, Civil Rights, and Civil Liberties Audit Guidance for the State, Local, Tribal, and Territorial Intelligence Component***, Global, BJA, OJP, DOJ, September 30, 2015, https://it.ojp.gov/GIST/181/Privacy--Civil-Rights--and-Civil-Liberties-Audit-Guidance-for-the-State--Local--Tribal--and-Territorial-Intelligence-Component.

- ***Recommendations for First Amendment-Protected Events for State and Local Law Enforcement Agencies***, Global, BJA, OJP, DOJ, October 13, 2011, https://it.ojp.gov/GIST/35/Recommendations-for-First-Amendment-Protected-Events-for-State-and-Local-Law-Enforcement-Agencies.

- ***Scenarios for PII Identification and Handling*, Appendix A, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)***, NIST, NIST Special Publication 800-122, April 2010, http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-122.pdf.

D. Acknowledgements

The information contained in this template does not represent the views, opinions, official position, or policies of any sole contributor or agency. Rather, this resource was created through a dynamic and collaborative effort of multiple state, local, and federal law enforcement, privacy, and criminal justice partners, practitioners, and subject-matter experts (SMEs). A special thank-you to the following individuals and agencies that provided valuable contributions in the development and vetting of this resource.

1. Face Recognition Policy Group Members

Chair: **Dawn Diedrich**, Director, Office of Privacy and Compliance, Georgia Bureau of Investigation

Federal Partners

- U.S. Department of Homeland Security (DHS)
  - Office of Intelligence and Analysis, State, Local, Tribal, and Territorial (SLTT) Partner Engagement —**Kevin Saupp**, Director of State and Local Partner Engagement, and **Susan Bower**, Program Manager
  - Privacy Office—**Scott Mathews**, Senior Privacy Analyst for Intelligence
  - Office for Civil Rights and Civil Liberties—**Ayn Crawley**, Director, Civil Rights and Civil Liberties Institute, and **David Demski**, Technology Analyst
  - Homeland Security Information Network (HSIN)—**Maria Petrakis**, Policy Manager
  - Office of Biometric Identity Management (OBIM), part of the National Protection and Programs Directorate—**Anne May**, Program and Management Analyst, and **Brian Pittack**, Program and Management Analyst
  - U.S. Customs and Border Protection, Biometric Exit program—**Brandon Fauquet**, Manager and Program Analyst, Planning, Program Analysis, and Evaluation, Office of Field Operations
- U.S. Department of Justice (DOJ)
  - Bureau of Justice Assistance (BJA), Office of Justice Programs (OJP), DOJ—**John Markovic**, Senior Policy Advisor, Justice Information Sharing Team
  - U.S. Drug Enforcement Administration (DEA)
    - **George Johnson III**, Investigative Tech
    - **Bob Montgomery**, Technical Director, All Native Group
    - **Spring Williams**, Unit Chief, Office of Investigative Technology
  - Federal Bureau of Investigation (FBI)
    - FBI Criminal Justice Information Services (CJIS) Division
    - FBI Terrorist Screening Center (TSC)
    - FBI Office of General Counsel/Privacy and Civil Liberties Unit
  - Office of Privacy and Civil Liberties (OPCL)—**Beth Zelman,** Attorney Advisor
  - Office of the Director for National Intelligence (ODNI), Office of Civil Liberties, Privacy, and Transparency—**Eva Kleederman**, Deputy Chief, and **Brian Ince**, Senior Assistant Civil Liberties, Privacy, and Transparency Officer
- ODNI, Office of Partner Engagement, Information Sharing Environment (PE-ISE)—**Frank Pawlowski**, Senior Law Enforcement Advisor

Biometric Privacy SME

- **Pam Dixon**, Executive Director, World Privacy Forum and member of the Privacy and Policy Expert Group, Biometrics Institute

Fusion Centers

- **Lieutenant Ron Fisher** and **Eric Diggs**, Maryland Coordination and Analysis Center
- **Jimmy Gianato**, Director, Division of Homeland Security and Emergency Management, West Virginia, West Virginia Intelligence Fusion Center

State- and Local-Level Facial Recognition Practitioners

- **Commanding Officer Inspector Joseph Courtesis** and **Sergeant Edwin Coello**, Facial Recognition Program, New York Police Department Real Time Crime Center

- **Special Agent in Charge Terry Cowman**, Iowa Department of Public Safety (Association of State Criminal Investigative Agencies [ASCIA] representative)
- **Detective Sergeant First Class Mark Finnegan**, Information & Intelligence Analysis Bureau, Office of the Regional Operations and Intelligence Center, New Jersey State Police
- **Lieutenant Sam McGhee**, Professional Standards Section, Emergency Services Coordinator, Aurora, Colorado Police Department, (International Association of Chiefs of Police, Homeland Security Committee representative)
- **Major Brian Redd**, Utah Department of Public Safety (ASCIA representative)
- **Pam Scanlon**, Executive Director, Automated Regional Justice Information System

2. Other Contributors

The following individuals were not members of the Face Recognition Policy Group but contributed to the resource through conference calls, policy language development, and template review and vetting.

- **Nelson O. Bunn, Jr.**, Executive Director, National District Attorneys Association (NDAA)
- **Lieutenant Cora Gentry**, Identification Bureau, Arkansas State Police
- **Pete Langenfeld**, Section Manager, Digital Analysis and Identification Section, Michigan State Police
- **Mark Vargo**, States Attorney, Pennington County, Rapid City, South Dakota (NDAA Policy Committee representative)

II. Face Recognition Policy Development Template for State, Local, and Tribal Criminal Intelligence and Investigative Activities

A. Purpose Statement

1. **Why did the entity implement a face recognition program or establish access and use of a face recognition system?**

   Facial recognition technology involves the ability to examine and compare distinguishing characteristics of a human face through the use of biometric algorithms contained within a software application. This technology can be a valuable investigative tool to detect and prevent criminal activity, reduce an imminent threat to health or safety, and help in the identification of persons unable to identify themselves or deceased persons. The **[name of entity]** has **[implemented or, if applicable, established access and use of]** a face recognition **[program or, if applicable, system]** to support the investigative efforts of law enforcement and public safety agencies both within and outside **[state name]**.

2. **What is the purpose of establishing a face recognition policy (i.e., what does the entity hope to accomplish in adopting this policy)? Provide a succinct, comprehensive statement of purpose.**

   It is the purpose of this policy to provide **[name of entity]** personnel with guidelines and principles for the collection, access, use, dissemination, retention, and purging of images and related information applicable to the implementation of a face recognition (FR) program. This policy will ensure that all FR uses are consistent with authorized purposes while not violating the privacy, civil rights, and civil liberties (P/CRCL) of individuals.

   Further, this policy will delineate the manner in which requests for face recognition are received, processed, catalogued, and responded to. The Fair Information Practice Principles (FIPPs) form the core of the privacy framework for this policy.

   This policy assists **[name of entity]** and its personnel in:
   - Increasing public safety and improving state, local, tribal, territorial, and national security.
   - Minimizing the threat and risk of injury to specific individuals.
   - Minimizing the threat and risk of physical injury or financial liability to law enforcement and others responsible for public protection, safety, or health.

- Minimizing the potential risks to individual privacy, civil rights, civil liberties, and other legally protected interests.
- Protecting the integrity of criminal investigatory, criminal intelligence, and justice system processes and information.
- Minimizing the threat and risk of damage to real or personal property.
- Fostering trust in the government by strengthening transparency, oversight, and accountability.
- Making the most effective use of public resources allocated to public safety entities.

3. What are the entity's authorized uses for face recognition information?[8]

All deployments of the face recognition system are for official use only/law enforcement sensitive (FOUO/LES). The provisions of this policy are provided to support the following authorized uses of face recognition information.

[List any of the following that may be applicable and add any other authorized uses that apply to the entity. Note: Uses must be specifically authorized for your entity and must be in accordance with laws, statutes, policies, and procedures governing the entity.

- **A reasonable suspicion that an identifiable individual has committed a criminal offense or is involved in or planning criminal (including terrorist) conduct or activity that presents a threat to any individual, the community, or the nation and that the information is relevant to the criminal conduct or activity.**
- **An active or ongoing criminal or homeland security investigation.**
- **To mitigate an imminent threat to health or safety through short-term situational awareness surveillance or other means.**
- **To assist in the identification of a person who lacks capacity or is otherwise unable to identify him- or herself (such as an incapacitated, deceased, or otherwise at-risk person).**
- **To investigate and/or corroborate tips and leads.**
- **For comparison to determine whether an individual may have obtained one or more official state driver's licenses or identification cards that contain inaccurate, conflicting, or false information.**
- **To assist in the identification of potential witnesses and/or victims of violent crime.**
- **To support law enforcement in critical incident responses.]**

[For those entities using mobile face image capture devices, there may be narrowly tailored purposes for use. Insert the following language and list the purposes that are applicable, and any others that are relevant, to the entity:

Mobile face image searches may be performed only by an officer who has completed training and only during the course of an officer's lawful duties, in furtherance of a valid law enforcement purpose and in accordance with the conditions set forth in section F.7 (Refer to F. Use of Face Recognition Information, item 7). Some suggested valid law enforcement purposes include:

- **For persons who are detained for offenses that:**
  - **Warrant arrest or citation or**
  - **Are subject to lawful identification requirements and are lacking positive identification in the field.**
- **For a person who an officer reasonably believes is concealing his or her true identity and has a reasonable suspicion the individual has committed a crime other than concealing his or her identity.**
- **For persons who lack capacity or are otherwise unable to identify themselves and who are a danger to themselves or others.**
- **For those who are deceased and not otherwise identified.]**

[8] Entities should reference the classification of information established in entity policies and procedures.

B. Policy Applicability and Legal Compliance

1. What information is subject to the face recognition policy?

This policy was established to ensure that all images are lawfully obtained, including face recognition probe images obtained or received, accessed, used, disseminated, retained, and purged by the **[name of entity]. This policy also applies to:**

- Images contained in a known identity face image repository and its related identifying information,
- **The face image** searching process.
- Any results from face recognition searches that may be accessed, searched, used, evaluated, retained, disseminated, and purged by the **[name of entity].**
- Lawfully obtained probe images of unknown suspects that have been added to unsolved image files (refer to section L.3), pursuant to authorized criminal investigations.

2. Who is subject to the face recognition policy? Identify who must comply with the face recognition policy; for example, entity personnel, <u>participating agencies</u>, and private contractors.

All **[name of entity]** personnel, participating agency personnel, and authorized individuals working in direct support of **[name of entity]** personnel (such as interns), personnel providing information technology services to the **[name of entity]**, private contractors, and other authorized users will comply with the **[name of entity]**'s face recognition policy and will be required to complete the training referenced in section N.2. In addition, authorized **[name of entity]** personnel tasked with processing face recognition requests and submissions must also complete the specialized training referenced in section N.3. An outside agency, or investigators from an outside agency, may request face recognition searches to assist with investigations only if **[insert applicable requirement(s) from those recommended below or insert the entity's established requirements:**

- **Prior to making requests, the outside agency has a formalized agreement (e.g., a memorandum of understanding or an interagency agreement) between the [name of entity] and the outside agency and the agreement acknowledges that requesting investigators have an understanding of the training concepts listed in section N. Training, item 4.**
- **The outside agency first provides examples of its applicable policies (e.g., privacy) and acknowledges in writing that its requesting investigators have an understanding of the training concepts listed in section N. Training, item 4.**
- **The outside agency completes the [name of entity]'s training identified in section N. Training, item 4.**
- **The outside agency is a law enforcement agency that is making the request based on a valid law enforcement purpose that falls within the authorized uses listed in section A. Purpose Statement, item 3. and the requestor provides a case number and contact information (requestor's name, requestor's agency, address, and phone number) and acknowledges an agreement with the following statement:**

  The result of a face recognition search is provided by the [name of entity] only as an investigative lead and IS NOT TO BE CONSIDERED A POSITIVE IDENTIFICATION OF ANY SUBJECT. Any possible connection or involvement of any subject to the investigation must be determined through further investigation and investigative resources.]

3. How is the entity's face recognition policy made available to personnel, participating entities, and individual users (e.g., in print, online, etc.), and does the entity require acknowledgment, in writing, of receipt and agreement to comply with this policy?

The **[name of entity]** will provide a printed or electronic copy of this face recognition policy to all:

- **[name of entity]** and non-**[name of entity]** personnel who provide services
- Participating agencies
- Individual authorized users

The **[name of entity]** will require both a written acknowledgement of receipt of this policy and a written agreement to comply with this policy and its applicable provisions.

4. **This entity requires *personnel and participating information-originating and user agencies* to be in compliance with all applicable constitutional and statutory laws. What are the primary laws with which personnel and <u>participating agencies</u> must comply?**

   Cite the primary laws with which personnel and participating users must comply that protect privacy, civil rights, and civil liberties (P/CRCL) in the collection, receipt, access, use, dissemination, retention, and purging of face recognition information.

   This should include any statute enacted by state or local government regarding deployed <u>face recognition systems</u> by affiliated entities. It might also include relevant provisions of the U.S. Constitution and state constitutions; open records or sunshine laws; information breach notification laws; other laws, regulations, orders, opinions, or policies impacting or protecting P/CRCL; local ordinances; and relevant federal laws, such as the Driver's Privacy Protection Act and regulations. (For synopses of primary federal laws, refer to Appendix C, Listing of Federal Laws.)

   All **[name of entity]** personnel, participating agency personnel, and authorized individuals working in direct support of **[name of entity]** personnel (such as interns or volunteers), personnel providing information technology services to the **[name of entity]**, private contractors, agencies from which **[name of entity]** information originates, and other authorized users will comply with applicable laws and policies concerning P/CRCL, including, but not limited to **[include a specific reference to any relevant state statutes or other binding state or local policy specific to <u>face recognition systems</u>, then provide a list of other applicable state and federal P/CRCL laws and/or include a reference to the section or appendix containing a list of applicable laws]**.

C. Governance and Oversight

1. **Who has primary responsibility for the entity's overall operation, including the entity's justice information systems, face recognition program and system, information collection and retention procedures, coordination of personnel, and enforcement of this policy? Which individual will ultimately be held accountable for any problems or errors?**

   Primary responsibility for the operation of the **[name of entity]**'s justice information systems, face recognition program and system, operations, and the coordination of personnel; the receiving, seeking, retention, evaluation, data quality, use, purging, sharing, disclosure, or dissemination of information; and the enforcement of this policy is assigned to the **[position/title]** of the **[name of entity]**.

2. **Who is assigned primary responsibility for overseeing and administering the entity's <u>face recognition program</u>?**

   The **[name of entity]**'s **[insert title]** will designate **[a face recognition administrator or face recognition unit or department who/that]** will be responsible for the following **[include any of the following responsibilities that apply to the face recognition administrator or other responsibilities:**
   - **Overseeing and administering the face recognition program to ensure compliance with applicable laws, regulations, standards, and policy.**
   - **Acting as the authorizing official for individual access to face recognition information.**
   - **Ensuring that user accounts and authorities granted to personnel are maintained in a current and secure "need-to-know" status.**
   - **Reviewing face recognition search requests, reviewing the results of face recognition searches, and returning the most likely candidates—or candidate images—if any, to the requesting agency.**

- **Ensuring that protocols are followed to ensure that face recognition information (including probe images) is automatically purged in accordance with the entity's retention policy (refer to section L.1. Information Retention and Purging), unless determined to be of evidentiary value.**
- **Ensuring that random evaluations of user compliance with system requirements and the entity's face recognition policy and applicable law are conducted and documented (refer to section M.2. Accountability).**
- **Confirming, through random audits, that face recognition information is purged in accordance with this policy and to ensure compliance with applicable laws, regulations, standards, and policy.**
- **Ensuring and documenting that personnel (including investigators from external agencies who may make face recognition search requests) meet all prerequisites stated in this policy prior to being authorized to use the face recognition system.]**

3. **What is the operating entity's role with regard to the face recognition program?**

   [Select the option that is applicable to the entity.]

   Option 1: The entity operates its own face recognition program.

   The **[name of entity]** face recognition program was established on **[date]** in conjunction with **[other agency partners, if applicable]**. Personnel from the following agencies are authorized to request face recognition searches:
   - **[Insert list of agencies authorized to request face recognition searches]**.

   Option 2: The entity has authorized access to a face recognition system.

   The **[name of entity]** has authorized access to and can perform face recognition searches utilizing the **[insert name of entity that owns the face recognition program]** face recognition system.

4. **Is there is a commercial entity or vendor involved and, if so, what is that vendor's role?**

   The **[name of entity]** contracts with **[insert name of commercial entity or vendor]** to provide **[insert applicable vendor role, such as "software and system development services for the entity's face recognition system"]**. The **[name of entity]** retains ownership of the face recognition system and the images and information it contains.

5. **What is the process for developing, reviewing, and updating the face recognition policy?**

   The **[name of entity]** is guided by a **[insert guiding authority, for example, a "designated face recognition oversight committee"]** that ensures that P/CRCL are not violated by this face recognition policy and by the **[name of entity]**'s face recognition information collection, receipt, access, use, dissemination, retention, and purging processes and procedures. The **[insert guiding authority, for example, a "designated face recognition oversight committee"]** engages with the community regarding **[name of entity]'s** face recognition policy prior to publishing.

   It is suggested that the committee will annually review and update the face recognition policy in response to changes in law and program implementation experience, including the results of audits and inspections, and may ***solicit input from the entity's stakeholders*** **[insert, if applicable "and may provide notice to and solicit comment from the public"]** on the development of the face recognition policy or proposed updates to the face recognition policy.

6. **Who is the designated and trained privacy officer (or entity) who will handle reported errors and violations of this policy and who will oversee the implementation of this policy and face recognition P/CRCL protections?**

[Provide the title of the individual or name of the entity. This may be the privacy officer; legal counsel; internal affairs; external entities such as the U.S. Attorney or the Office of Inspector General; or other personnel who have independent authority to perform oversight responsibilities.]

The **[insert title of individual or name of entity]** will:

- Receive reports regarding alleged errors and violations of the provisions of this face recognition policy or applicable state law.
- Receive and coordinate complaint resolution under the [name of entity]'s face recognition redress policy.
- Ensure that the provisions of this policy and P/CRCL protections are implemented through efforts such as training, business process changes, and system designs that incorporate privacy-enhancing technologies.

The **[insert title of individual but not the name or name of entity]** may be contacted at the following address: **[insert phone number, mailing address, or e-mail address]**, which is also posted on **[insert website where this information is listed for purposes of public redress]**.

7. **Who, or what entity, is responsible for ensuring that enforcement procedures and sanctions for noncompliance with the face recognition policy are adequate and enforced?**

   The **[insert title of individual or name of entity]** will ensure that enforcement procedures and sanctions outlined in **[insert section number of policy (see Section M.3. Enforcement)]** are adequate and enforced.

D. Definitions

1. **What key words or phrases are regularly used in the face recognition policy for which the entity wants to specify particular meanings?**

   This may include terms that are not commonly known or have multiple meanings that may need to be clarified to indicate which one applies to the face recognition policy. There may be legal definitions for terms in the statutes governing the operation of justice information or face recognition systems or programs. For examples of definitions of key terms commonly used throughout this template, refer to Appendix A, Glossary of Terms and Definitions.

   For examples of primary terms and definitions used in this face recognition policy, refer to **[insert section or appendix citation]**.

E. Acquiring and Receiving Face Recognition Information

1. **What image repositories are searched using the entity's <u>face recognition system</u>? Select all options that are applicable to the entity.**

   Option 1: The entity maintains or operates an entity-owned image <u>repository</u>.

   The **[name of entity]** face recognition system can access and perform face recognition searches utilizing the following entity-owned face image repositories:

   - **[Insert a list of entity-owned and maintained repositories, including information types.]**

Option 2: The entity has authorized access to and can perform face recognition searches utilizing image repositories not owned by the entity. Indicate the authority/source of the repository (e.g., driver's license images).

The **[name of entity]** is authorized to access and perform face recognition searches utilizing the following external repositories:

[List the image type and authority/source for each repository accessed. These may include:

- **Mug-shot images [check state authority and insert source]**
- **Driver's license photographs [check state authority and insert source]**
- **State identification card photographs [check state authority and insert source]**
- **Sex Offender Registry [check state authority and insert source]**
- **[Specify any other image repositories that are accessed and cite state authority.]]**

Option 3: In addition to the above, the entity is authorized to request that face recognition searches be performed by an external entity that operates a face recognition program.

In addition to above, the **[name of entity]** is authorized to submit requests for face recognition searches to be performed by the following external entities that own and maintain face image repositories:

[List the image type and authority/source for each repository accessed. These may include:

- **Mug-shot images [check relevant state law and insert source]**
- **Driver's license images [check relevant state law and insert source]**
- **State identification card images [check relevant state law and insert source]**
- **Sex Offender Registry [check relevant state law and insert source]**
- **[Specify any other image repositories that are accessed and cite state authority.]]**

2. **For use in performing a face recognition search, describe the conditions under which the entity will obtain or accept probe images. Note: State and federal law and/or policies may restrict queries to commercial repositories.**

   For the purpose of performing face recognition searches, the **[name of entity]** and authorized **[name of entity]** personnel will obtain probe images or accept probe images from authorized requesting or participating agencies only for the authorized uses identified in A. 2.

3. **If the entity receives probe images from other law enforcement agencies, identify the mechanism by which this occurs (e.g., memorandum of understanding [MOU], law, intergovernmental agreement [IGA]).**

   The **[name of entity]** will receive probe images only from **[list other law enforcement agency or agencies]** in accordance with **[insert mechanisms, e.g., MOU, law, intergovernmental or interagency agreement]** established between the **[name of entity]** and the law enforcement agency(ies). If a non-law enforcement entity wants to submit a probe image for the purpose of a face recognition search, the entity will be required to file a criminal complaint with the appropriate law enforcement entity prior to the search.

4. **Identify the federal or state constitutional prohibitions or prohibitions in federal, state, local, or tribal laws under which the entity and/or participating agencies will not request or perform face recognition searches.**

   Best Practice: Entities should consider an additional level of review and approval in order to enhance protection and ensure appropriate use of this technology in sensitive locations or populations.

The **[name of entity]** and, if applicable, any authorized requesting or participating agencies will not violate First, Fourth, and Fourteenth Amendments and will not perform or request face recognition searches about individuals or organizations based solely on their religious, political, or social views or activities; their participation in a particular noncriminal organization or lawful event; or their races, ethnicities, citizenship, places of origin, ages, disabilities, genders, gender identities, sexual orientations, or other classification protected by law.

However, the **[name of entity]** accords special consideration to the collection of face images relating to First Amendment-protected events, activities, and affiliations. Because of the sanctity of the First Amendment, law enforcement's role at First Amendment-protected events is usually limited to crowd control and public safety.[9] If, however, during the planning assessment and approval process for the particular event, before proceeding with the collection, the **[name of entity]** anticipates a need for the collection of face images, the **[name of entity]** will articulate whether collection of face images by law enforcement officers at the event is permissible; the legal or justified basis for such collection (including specifics regarding the criminal behavior that is suspected); and how face images may be collected, used, or retained, in accordance with this policy, as appropriate. If face images will be collected, the plan will specify the type of information collection that is permissible, identify who will collect face images (uniform or plainclothes officers), and define the permissible acts of collection.

[Note: Some law enforcement purposes may be stated generally in the Operations Plan or communicated to officers, but objectives that may risk interference with the exercise of First Amendment rights should be stated narrowly and be expressly tied to a specific law enforcement function (e.g., public safety, investigative).]

The use of mobile face image capture devices relating to First Amendment-protected events, activities, and affiliations will be specially authorized by **[title of entity supervisor/director/administrator]** of the **[name of entity]** in advance of the event.

The **[name of entity]** will reassess the need for and use of face recognition during the First Amendment-protected event. The **[name of entity]** will utilize face images from a First Amendment-protected event should the public safety mission change or in support of an active or ongoing criminal or homeland security investigation that occurs during or resulted from a First Amendment-protected event.

5. **If the entity contracts with a commercial face recognition vendor, does the entity require an assurance that the vendor or subcontractor is in legal compliance in its information collection, receipt, access, retention, dissemination, and purging procedures?**

   The **[name of entity]** will contract only with commercial face recognition companies or subcontractors that provide assurances that their methods for collecting, receiving, accessing, disseminating, retaining, and purging face recognition information comply with applicable local, state, tribal, territorial, and federal laws, statutes, regulations, and policies and that these methods are not based on unfair or deceptive information collection practices.

F. Use of Face Recognition Information

1. **Describe the authorized access to or disclosure of face recognition search results *within the entity or in other governmental agencies*. Entities may consider developing policies for addressing use of face recognition in conjunction with certain "sensitive" locations or populations (e.g., places of worship, academia). In addition, indicate if the entity has certain restrictions or allowances for the use of images in briefings or trainings, and whether there are any distinctions for hard copy versus digital images.**

[9] For further information about these processes, see *Recommendations for First Amendment-Protected Events for State and Local Law Enforcement Agencies* at 4, Global Justice Information Sharing Initiative, https://it.ojp.gov/GIST/35/Recommendations-for-First-Amendment-Protected-Events-for-State-and-Local-Law-Enforcement-Agencies.

Best Practice: Entities should consider an additional level of review and approval in order to enhance protection and ensure appropriate use of this technology in sensitive locations or populations.

Access to or disclosure of face recognition search results will be provided only ***to individuals within the entity or in other governmental agencies*** who are authorized to have access and have completed applicable training outlined in section N. Training, and only for valid law enforcement purposes (e.g., enforcement, reactive investigations), and to IT personnel charged with the responsibility for system administration and maintenance. Authorized uses are described in A.3 of this policy. [**Insert, if applicable, any additional restrictions or allowances regarding the use of images in briefings or trainings, and whether there are any distinctions for hard-copy versus digital images.]**

2. **For what purposes does the entity prohibit accessing and using the face recognition system and disseminating face recognition search results?**

The **[name of entity]** will prohibit access to and use of the face recognition system, including dissemination of face recognition search results, for the following purposes:

- Non-law enforcement (including but not limited to personal purposes).
- Any purpose that violates the U.S. Constitution or laws of the United States, including the protections of the First, Fourth, and Fourteenth Amendments.
- Prohibiting or deterring lawful individual exercise of other rights, such as freedom of association, implied by and secured by the U.S. Constitution or any other constitutionally protected right or attribute.
- Harassing and/or intimidating any individual or group.
- Any other access, use, disclosure, or retention that would violate applicable law, regulation, or policy.

3. **Does the entity allow face recognition analysis on live or recorded video?**

Best Practice: It is important for the entity to articulate a clear and affirmative statement regarding the entity's position regarding face recognition analysis on live or recorded video.[10]

The **[name of entity] [does not/does]** connect the face recognition system to any interface that performs live video surveillance, including surveillance cameras, drone footage, and body-worn cameras. The face recognition system **[will not/will]** be configured to conduct face recognition analysis on live or recorded video.

4. **What types of user actions and permissions are controlled by the entity's face recognition access limitations?**

Best Practice: Least privilege administration is a recommended security practice in which every user is provided with only the minimum privileges needed to accomplish the tasks he or she is authorized to perform. It is suggested that entities specify their method for identifying user actions and permissions as it relates to face recognition information within their face recognition policies.

The **[name of entity]** will employ credentialed, role-based access criteria, as appropriate, to control:

- Categories of face recognition information to which a particular group or class of users may have access, based on the group or class.
- The assignment of roles (e.g., administrator, manager, operator, and user).
- The categories of face recognition information that a class of users are permitted to access, including information being utilized in specific investigations.

[10] Face recognition analysis on live video is different than mobile face recognition. While mobile recognition entails using a mobile device to capture a photo of a subject who is in the presence of a law enforcement officer (e.g., during a traffic stop), face recognition analysis on live video means that face recognition searches may be performed on images of any individual captured within the frame of a live feed video camera (such as a closed circuit television).

- Any administrative or functional access required to maintain, control, administer, audit, or otherwise manage the information or equipment.

5. **What is the entity's standard face recognition search procedure?**

   The following is a suggested sample procedure which should be customized by the entity to reflect its actual face recognition search standard procedures. Each agency will determine which of the following steps, and others, are necessary to support its various operations, acknowledging that each step may not be executed (e.g., using a filtered search as a secondary search) in every instance.

   Note: Entities are encouraged to refer to the National Institute of Standards and Technology's (NIST) Face Recognition Vendor Test (FRVT) Ongoing website for information on matching algorithms from independent government evaluations of commercially available and prototype face recognition technologies at https://www.nist.gov/programs-projects/face-recognition-vendor-test-frvt-ongoing.

   The following describes the **[name of entity]**'s manual and automated face recognition search procedure, which is conducted in accordance with a valid law enforcement purpose and this policy.
   - Authorized **[name of entity]** personnel **[and/or authorized requesting agency personnel]** will submit a probe image of a subject of interest.
   - Trained **[name of entity]** authorized examiners will initially run probe images without filters, using a filtered search as a secondary search, if needed. In some cases, enhancements may be considered after running an image as is against the image repository.
   - In the automated search, most likely candidates are returned to the requestor ranked in order based on the similarity or confidence level.
   - The resulting candidates, if any, are then manually compared with the probe images and examined by an authorized, trained examiner. Examiners shall conduct the comparison of images, biometric identifiers, and biometric information in accordance with their training.
     - If no likely candidates are found, the requesting entity will be informed of the negative results. In the case of a negative result, the images examined by the examiner will not be provided to the requesting entity.
   - Examiners will submit the search and subsequent examination results for a peer review of the probe and candidate images for verification by other authorized, trained examiners.
   - All results of most likely candidate images from the face recognition search must be approved by a supervisor prior to dissemination.
   - All entities receiving the results of a face recognition search, must be cautioned that the resulting candidate images do not provide positive identification of any subject, are considered advisory in nature as an investigative lead only, and do not establish probable cause, without further investigation, to obtain an arrest warrant without further investigation.
   - The following statement will accompany the released most likely candidate image(s) and any related records:

     The **[name of entity]** is providing this information as a result of a search, utilizing face recognition software, of records maintained by the **[name of records entity]**. This information is provided only as an investigative lead and **IS NOT TO BE CONSIDERED A POSITIVE IDENTIFICATION OF ANY SUBJECT**. Any possible connection or involvement of any subject to the investigation must be determined through further investigation and investigative resources.

6. **Does the entity operate a mobile face recognition search capability and, if so, what is the process?**

   The **[name of entity]** has established the following process for mobile face recognition searches:
   - Only **[name of entity]** authorized and trained officers may utilize the mobile face recognition application and only on department-authorized devices. **[If personal devices are permitted, insert entity policy regarding use of mobile face recognition on personal devices.]**

- Prior to utilizing a face recognition search, an officer should first attempt to ascertain an individual's identity by means other than a face recognition search, such as requesting identification, using a fingerprint scanner, etc.
- Mobile searches may be performed during the course of an officer's lawful duties and only for the entity-established authorized uses listed in section A. Purpose Statement, item 3.
- In addition, officers may only capture an individual's image when one of the conditions listed in section F.7 exist.
- **[Use the following language, if the process is applicable to the entity. "The face recognition system does not work over standard cellular internet. Officers must log in and be authenticated into the [name of entity]'s law enforcement network in order to access the face recognition system."]**
- The log-in screen will prompt the user to acknowledge and agree to the following statement before granting access to the system:
  - Face recognition is not a form of positive identification of a subject. Images returned as a result of a face recognition search may be considered investigative lead information only and are not probable cause to arrest, without further investigation.
  - Face recognition searches shall not be performed by the user on behalf of others who have not been trained and authorized to perform the searches.
  - All face recognition searches are subject to audit and require case numbers and file class/crime types.
  - Misuse may result in administrative and/or criminal penalties.
- Prior to executing the search, the officer must enter the reason for the search within the application. **[List the reasons that are prompted by the entity's face recognition application. Reasons may include the following:**
  - **Consent**
  - **Reasonable suspicion of a crime**
  - **Probable cause**
  - **Physical/mental incapacity**
  - **Test/training**
  - **Other—[enter written reason]**
- The captured image (probe image) will be submitted to the face recognition system, which will compare the probe image with those contained in the **[indicate the name(s) of repository/ies searched]**.
- A list of most likely candidate images is returned ranked by computer-evaluated similarity.
- The officer then completes a visual or manual morphological comparison of the candidate images with the subject's probe image to make a visual judgment, as well as uses standard investigative techniques, to determine whether the subject is the same as a candidate image.

7. What are the conditions by which a mobile face recognition search may be conducted?

Authorized and trained **[name of entity]** officers may only perform a mobile face recognition search during the course of lawful duties, in accordance with entity-established authorized uses (refer to section A. Purpose Statement, item 3), and when one of the following conditions exist:

- Public Place: In accordance with applicable law, the individual's image is captured in a public place for the purpose of identification and the individual has no reasonable expectation of privacy. The **[name of entity]** will not authorize the collection of the individual's face image when the individual raises an objection that is recognized by law (e.g., religious objection).
- Consent: The individual consents to have his or her image captured for the purpose of identification. The individual may withdraw consent at any time. If consent is withdrawn and neither of the other conditions applies, then use of a face recognition search is not authorized and the search must stop immediately.
- Incapacitation, Defect, or Death: When an individual is unable to provide reliable identification because of physical incapacitation or defect, mental incapacitation or defect, or death, and an immediate identification is needed to assist the officer in the performance of his or her lawful duties.

8. **When, if ever, is force used to capture a subject's image?**

   At no time is the use of force permitted to capture a subject's image.

G. Sharing and Disseminating Face Recognition Information

1. **What requirements must be met before external law enforcement agencies can request face recognition searches?**

   The **[name of entity]** will establish requirements for external law enforcement agencies to request face recognition searches. These will be documented in an interagency agreement or MOU, which will include an assurance from the external agency that it complies with the laws and rules governing it, including applicable federal and state laws. The agreement will specify only those agency personnel who have been authorized by the **[name of entity]**, who have completed the required training identified in section N.2, and that requests are for official use only/law enforcement sensitive (FOUO/LES). Each request must be accompanied by a complaint number or case number.

2. **Under what circumstances will the entity or contracted vendor *not disclose* face recognition information?**

   The **[name of entity]**'s face recognition search information **will not** be:
   - Sold, published, exchanged, or disclosed to commercial or private entities or individuals except as required by applicable law and to the extent authorized by the **[name of entity]**'s agreement with the commercial vendor.
   - Disclosed or published without prior notice to the originating entity that such information is subject to disclosure or publication. However, the **[name of entity]** and the originating agency may agree in writing in advance that the **[name of entity]** will disclose face recognition search information as part of its normal operations, including disclosure to an external auditor of the face recognition search information.
   - Disclosed on a discretionary basis unless the originating agency has provided prior written approval or unless such disclosure is otherwise authorized by the MOU or agreement between the **[name of entity]** and the originating agency.
   - Disclosed to unauthorized individuals or for unauthorized purposes.
   - **[For commercial face recognition vendors, the entity should closely review its vendor agreement.]**

3. **State the entity's policy on confirming the existence or nonexistence of face recognition information to individuals or agencies that are not authorized to receive the information.**

   Note: This provision is unrelated to policy transparency and is not intended to imply that entities not make their face recognition policies available to the public. Rather, this template promotes entity face recognition policy transparency. Refer to Chapter 1. Introduction, Section B. How to Use This Resource, item 3. Transparency and Referencing Other Policies, for guidance on this subject. In addition, refer to section M. Accountability and Enforcement, subsection M.1. Transparency, item 1 within this chapter for the policy provision addressing entity policy transparency.

   The **[name of entity]** will not confirm the existence or nonexistence of face recognition information to any individual or agency that would not be authorized to receive the information unless otherwise required by law.

H. Data Quality Assurance

1. **What is the entity's policy for ensuring that the original image is not altered, changed, or modified?**

   Original probe images will not be altered, changed, or modified in order to protect the integrity of the image. Any enhancements made to a probe image will be made on a copy, saved as a separate image, and documented to indicate what enhancements were made, including the date and time of change.

2. **Does the entity review the quality and suitability of probe images prior to performing a face recognition search?**

   [Name of entity] examiners will analyze, review, and evaluate the quality and suitability of probe images, to include factors such as the angle of the face image, level of detail, illumination, size of the face image, and other factors affecting a probe image prior to performing a face recognition search.

3. **What is the entity's policy regarding use of the face recognition search results for law enforcement action?**

   The **[name of entity]** considers the results, if any, of a face recognition search to be advisory in nature as an investigative lead only. Face recognition search results are **not** considered positive identification of a subject and do not, on their own, establish probable cause, without further investigation. Any possible connection or involvement of the subject(s) to the investigation must be determined through further investigative methods.

   [Add the following statement if the entity utilized mobile face recognition searches.

   All potential matches are considered advisory in nature and any subsequent verification of the individual's identity, such as through a fingerprint check, or follow-on action should be based on an agency's standard operating procedures.]

4. **What is the entity's procedure for ensuring proper face recognition system performance? Routine testing of the face recognition system build, or enhancement, should be performed to ensure the system is operating as designed, continuously available to users without malfunctions or deficiencies, and delivering search results within the accuracy rate of the specific system requirement. Testing also confirms, when system enhancements are made, whether they result in improved performance, (e.g., increased accuracy, speed, filtered search capabilities).**

   The **[name of entity]** will make every reasonable effort to perform routine maintenance, upgrades and enhancements, testing, and refreshes of the face recognition system to ensure proper performance, including the following:
   - Designated, trained personnel shall assess the face recognition system on a regular basis to ensure performance and accuracy.
   - Malfunctions or deficiencies of the system will be reported to the **[insert position/title]** within **[insert time period, e.g., number of days]** of discovering the malfunctions or deficiencies.

5. **Does the entity research alleged errors and malfunctions or deficiencies of face recognition information (or requests that the originating agency or vendor investigates)?**

   The integrity of information depends on quality control and correction of recognized errors which is key to mitigating the potential risk of misidentification or inclusion of individuals in a possible identification. The **[name of entity]** will investigate, in a timely manner, alleged errors and malfunctions or deficiencies of face recognition information or, if applicable, will request that the originating agency or vendor investigate the alleged errors and malfunctions or deficiencies. The **[name of entity]** will correct the information or advise the process for obtaining correction of the information.

I. Disclosure Requests

1. **Does the entity provide face recognition information *to a member of the public* in response to a request based on state open records, sunshine law, or the Freedom of Information Act (FOIA)? For this policy provision, consult with legal counsel to determine under what conditions, if any, face recognition information would be disclosed to a member of the public.**

   Notes:
   - **This issue does not apply to circumstances in which an entity chooses to provide sensitive information in accordance with entity policy in response to an emergency situation or provide nonsensitive information to the public.**
   - **Personal biometric data is generally inaccessible under FOIA. Additional information surrounding face recognition systems and policies may be accessible pursuant to FOIA and state open government laws.**

   Face recognition information will be disclosed to the public in accordance with **[cite applicable state retention laws, public records laws, and policy]**. A record will be kept of all requests and of what information is disclosed to an individual. **[If the state law prohibits disclosure, revise provision to reflect this.]**

J. Redress

J.1 Complaints

1. **What is the entity's procedure for handling individuals' complaints with regard to face recognition information received, maintained, disclosed, or disseminated by the entity?**

   If an individual has a complaint with regard to face recognition information that is exempt from disclosure, is held by the **[name of entity]**, and allegedly has resulted in demonstrable harm to the complainant, the **[name of entity]** will inform the individual of the procedure for submitting (if needed) and resolving such complaints. Complaints will be received by the entity's **[Privacy Officer, Face Recognition Administrator, Internal Affairs Representative, or other position title]** at the following address: **[insert mailing address, e-mail address, and/or link to page if complaints can be submitted electronically]**. The **[Privacy Officer, Face Recognition Administrator, Internal Affairs Representative, or other position title]** will acknowledge the complaint and state that it will be reviewed but will not confirm the existence or nonexistence of the information to the complainant unless otherwise required by law.

   If the face recognition information did not originate with the entity, the **[Privacy Officer, Face Recognition Administrator, Internal Affairs Representative, or other position title]** will notify the originating agency within 30 days in writing or electronically and, upon request, assist such agency to correct any identified data/record deficiencies in the information or verify that the record is accurate.

   All face recognition information held by the entity that is the subject of a complaint will be reviewed within 30 days and confirmed or corrected/purged if determined to be inaccurate or incomplete, to include incorrectly merged or out-of-date information. If there is no resolution within 30 days, the entity will not share the information until such time as the complaint has been resolved. A record will be kept by the entity of all complaints and the resulting action taken in response to them.

J.2 Requests for Corrections

1. **If, in accordance with state statute, the entity is subject to disclosure, what is the entity's procedure for handling individuals' requests for correction involving *face recognition information it can change because it originated the information*? Is a record kept of requests for corrections?**

   If, in accordance with state law, an individual requests correction of face recognition information *originating with the* **[name of entity]** that has been disclosed, the **[name of entity]**'s **[insert title of designee]** will inform the individual of the procedure for requesting a correction. The **[name of entity]** will investigate, in a timely manner, alleged errors and malfunctions or deficiencies of face recognition information or, if applicable, will request that the originating agency or vendor investigate the alleged errors and malfunctions or deficiencies. The **[name of entity]** will correct the information or advise the process for obtaining correction of the information. A record will be kept of all requests and the **[name of entity]**'s response.

J.3 Appeals

1. **If requests for disclosure or corrections are denied, what is the entity's procedure for appeal? Refer to state public records laws and explain the appeals process, including the identity of the office or officer charged with enforcing the public records act; the mailing or e-mail address of the office or officer charged with this responsibility; the time frame for filing the appeal; and the requisite documentation that must be submitted (e.g., a copy of the request, a copy of the response, and a written statement explaining why the requestor asserts that the record is a public record).**

   The individual who has requested disclosure or to whom face recognition information has been disclosed will be informed of the reason(s) why the **[name of entity]** or originating agency denied the request for disclosure or correction. The individual will also be informed of the procedure for appeal when the **[name of entity]** or originating agency has cited an exemption for the type of information requested or has declined to correct challenged face recognition information to the satisfaction of the individual to whom the information relates.

K. Security and Maintenance

1. **What are the entity's physical, procedural, and technical safeguards for ensuring the security and privacy of face recognition information?**

   Describe how the entity will protect the face recognition information from compromise, such as:
   - **Unauthorized access**
   - **Modification**
   - **Theft**
   - **Sabotage (whether internal or external)**
   - **Natural or human-caused disasters**
   - **Intrusions**
   - **Deletion**

   Consider procedures, practices, system protocols, use of software, information technology tools, and physical security measures.

   <u>Best Practice</u>: Reference generally accepted industry or other applicable standard(s) for security with which the entity complies (e.g., National Institute of Standards and Technology guidance).

   The entity will comply with generally accepted industry or other applicable standards for security, in accordance with **[insert the name of the entity security policy or reference applicable standard(s)]** to protect data at rest, in motion, or in use. Security safeguards will cover any type of medium (printed or

electronic) or technology (e.g., physical servers, virtual machines, and mobile devices) used in a work-related **[name of entity]** activity.

The **[name of entity and, if applicable, the name of entity's face recognition vendor]** will operate in a secure facility protected with multiple layers of physical security from external intrusion and will utilize secure internal and external security and privacy safeguards against network intrusions, such as strong multifactor authentication; encrypted communications; firewalls; and other reasonable physical technological, administrative, procedural, and personnel security measures to minimize the risks of unauthorized access to the system. Access to **[name of entity]** face recognition information from outside the facility will be allowed only over secure networks.

All results produced by the [name of entity] as a result of a face recognition search are disseminated by secured electronic means (such as an official government e-mail address). Non-electronic disseminations will be conducted personally or by phone with the requestor or designee.

2. What are the entity's procedures for adhering to data breach notification laws or policies?

All individuals with access to **[name of entity]**'s information or information systems will report a suspected or confirmed breach to the **[Privacy Officer, Face Recognition Administrator, or other position title]** as soon as possible and without unreasonable delay, consistent with applicable laws, regulations, policies, and procedures. This includes a breach in any medium or form, including paper, oral, and electronic.

Best Practice: Provide prompt notification to originating agencies when face recognition information they provided to the entity has been the subject of a suspected or confirmed data breach.

[To the extent allowed by existing data breach notification law] Following assessment of the suspected or confirmed breach and as soon as practicable, the **[name of entity]** will notify the originating agency from which the entity received face recognition information of the nature and scope of a suspected or confirmed breach of such information.

[In addition to the above, the entity should identify any existing laws or policies governing its breach response procedures and, in accordance with these laws and policies, provide specific guidance on breach response procedures, including notification to individuals affected by the breach. Determine whether your state has a data breach notification law and select the appropriate provision.]

Option 1: State, Local, Tribal, or Territorial Data Breach Notification Law

The **[name of entity]** adheres to **[insert citation to applicable data breach notification law.]**. The **[name of entity]** will determine whether a data breach requires notification to an affected individual, in accordance with applicable laws, regulations, policies, and procedures.

Option 2: Office Management and Budget (OMB) Memorandum M-17-12, Preparing for and Responding to a Breach of Personally Identifiable Information (January 13, 2017), https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2017/m-17-12_0.pdf. For additional information on the development of incident response plans, entities may refer to DOJ's *Best Practices for Victim Response and Reporting of Cyber Incidents*, https://www.justice.gov/sites/default/files/opa/speeches/attachments/2015/04/29/criminal_division_guidance_on_best_practices_for_victim_response_and_reporting_cyber_incidents2.pdf.

[Where no applicable state, local, tribal, or territorial law exists, or where entities choose to supplement existing law or policy, M-17-12 may be used as a guide. Entities do not need to adopt OMB M-17-12 in full. Rather, entities should review OMB M-17-12

to determine which provisions are applicable and may adapt those provisions to the specific needs of the entity.]

The **[name of entity]** will adhere to breach procedures established by Office Management and Budget (OMB) Memorandum M-17-12 (January 13, 2017). The provisions adopted by the **[name of entity]** are cited below. In accordance with OMB M-17-12 **[insert citations to the sections and paragraphs of OMB M-17-12 that will be adopted]** and relevant laws, regulations, policies, and procedures, the **[name of entity]** will determine if, when, and how to provide notification to potentially affected individuals and other relevant entities.

Option 3: No State Data Breach Notification Law and Entity Does Not Follow OMB M-17-12

a. Entity Follows an Existing Data Breach Notification Policy

The **[name of entity]** will adhere to the **[name of entity]**'s policy governing data breach notification. In accordance with **[insert citation(s) to the existing policy and procedures]**, the **[name of entity]** will **[insert excerpted language from the policy and procedures, as appropriate here]**. The **[name of entity]** will determine whether a data breach requires notification to an affected individual, in accordance with applicable laws, regulations, policies, and procedures.

b. Entity Does Not Have an Existing Data Breach Notification Policy

[Review and adapt the following template language to reflect the entity's data breach notification policy and procedures.]

When the **[Privacy Officer, Face Recognition Administrator, or other position title]** is notified of a suspected or confirmed breach, the **[Privacy Officer, Face Recognition Administrator, or other position title]** will determine whether the entity's response can be conducted at the staff level or whether a breach response team, consisting of the **[Privacy Officer, Face Recognition Administrator, or other position title, and others (e.g., individual with oversight responsibility for entity operation, the entity security officer, legal counsel, privacy oversight committee, and/or other designee(s))]** must be convened to respond to the breach. The **[Privacy Officer, Face Recognition Administrator, or other position title]**, in coordination with the breach response team, when applicable, will assess the risk of harm to individuals potentially affected by a breach (e.g., the nature and sensitivity of the personally identifiable information [PII] potentially compromised by the breach, the likelihood of access and use of PII, and the type of breach involved), evaluate how the entity may best mitigate the identified risks, and provide recommendations to the **[title of individual with oversight responsibility for entity operation]** on suggested countermeasures, guidance, or other actions.

The **[title of individual with oversight responsibility for entity operation]** will determine whether a data breach requires notification to an affected individual, in accordance with applicable laws, regulations, policies, and procedures. If required, the **[name of entity]** will notify an individual whose PII was or is reasonably believed to have been breached and access to which threatens physical, reputational, or financial harm to that person. If notice to the individual is required, it will be made promptly and without unreasonable delay following discovery of the breach. Notice will be provided consistent with the legitimate needs of law enforcement to investigate the breach or any measures necessary to determine the scope of the breach and, if necessary, to reasonably restore the integrity of any information system affected by the breach.

The **[Privacy Officer, Face Recognition Administrator, or other position title]** is responsible for developing and updating the entity's data breach response plan on an annual basis and in accordance with any changes in law, guidance, standards, agency

policy, procedures, staffing, and/or technology; for maintaining documentation about each data breach reported to the entity and the entity's response; and for keeping entity administrators informed of the status of an ongoing response. The **[title of individual with oversight responsibility for entity operation]** will determine when the response to a breach is concluded, based on input from the **[Privacy Officer, Face Recognition Administrator, or other position title]**.

3. **Is the entity's face recognition system maintained in compliance with the manufacturer's recommendations?**

   All face recognition equipment and face recognition software and components will be properly maintained in accordance with the manufacturer's recommendations, including routine updates as appropriate.

4. **What requirements exist to ensure that the face recognition information will be stored in a secure format and secure environment?**

   The **[name of entity or, if applicable, the name of the entity's face recognition vendor]** will store face recognition information in a manner that ensures that it cannot be modified, accessed, or purged except by personnel authorized to take such actions.

5. **What are the requirements for authorizing personnel to have access to the entity's face recognition system?**

   Authorized access to the **[name of entity]'s** face recognition system will be granted only to personnel whose positions and job duties require such access and who have successfully completed a background check and the training referenced in section N. Training.

6. **Does the entity prohibit sharing of passwords?**

   Usernames and passwords to the face recognition system are not transferrable, must not be shared by **[name of entity]** personnel, and must be kept confidential.

7. **Does the entity require specific configuration of strong passwords and require the replacement of manufacturer default passwords for all web-based system access within a specified time frame?**

   The system administrator will ensure that all manufacturer-generated default passwords are replaced with secure passwords before web-based interfaces of the system become operational. User passwords must meet the following standards **[insert rules, such as no English words and a combination of upper and lowercase letters, numbers, and at least two special characters]**. Authorized users are not permitted to use the same password over time and are required to change their password every **[insert period of time]**.

8. **Does electronic access to the entity's face recognition system identify the user? Is the identity of the user retained in the audit log?**

   Queries made to the **[name of entity]**'s face recognition system will be logged into the system identifying the user initiating the query. All user access, including participating agency access, and queries are subject to review and audit.

9. **Is a log kept of accessed and disseminated entity-owned face recognition information, and is an audit trail maintained? Refer to section M.2. Accountability, for more information on audit logs.**

   The **[name of entity]** will maintain an audit trail of requested, accessed, searched, or disseminated **[name of entity]**-held face recognition information. An audit trail will be kept for a minimum of **[specify the retention period for your jurisdiction/entity for this type of request]** of requests, access, and

searches of face recognition information for specific purposes and of what face recognition information is disseminated to each individual in response to the request.

Audit logs will include:
[Provide a list of the information maintained in the audit log, such as:

- **The name, agency, and contact information of the law enforcement user**
- **The date and time of access**
- **Case number**
- **Probe images (refer to section L.5)**
- **The specific information accessed**
- **The modification or deletion, if any, of the face recognition information**
- **The authorized law enforcement or public safety justification for access (criminal investigation, criminal intelligence, imminent threat, or identification), including a relevant case number if available. Note: The justification should be consistent with section E.]**

L. Information Retention and Purging

Agencies vary on their face recognition image retention policies regarding the specific laws and regulations of their jurisdictions and their strategic and tactical objectives in using the technology. Reference laws, if applicable. If images are stored in multiple repositories (mobile information computer [MDC]/laptops, mobile image capture devices, entity or nonentity servers, etc.), identify each repository and its associated retention period.

1. **What is the entity's retention policy for images contained in the entity's image repository?**

Notes:

- **The retention decision focuses on the face recognition record as a whole. Individual components of the face recognition record should not have different retention periods. However, if there are different categories of images that are retained, based on valid law enforcement purposes for retaining the images, include the retention policy for each category of images.**

  For example: "When, in accordance with an official law enforcement activity and this policy, face recognition searches are used for short-term situational awareness surveillance, the [name of entity] will purge face recognition images of nonviolators within [insert time period]. However, with respect to the retention of face recognition images relating to First Amendment-protected events, the [name of entity] limits the retention of face recognition images to [insert time period]."

- **In accordance with *Recommendations for First Amendment-Protected Events for State and Local Law Enforcement Agencies*,[11] "[a]gencies should limit the retention of information as much as possible to avoid the perception of maintaining files on groups or persons who engage in protected First Amendment activities."**

[Select all options that are applicable to the entity.]

Option 1: The entity maintains or operates an entity-owned image repository.

All images contained within the **[name of entity]**'s **[name of image repository, e.g., mug shot repository]** will be stored for a period not to exceed **[insert a time frame]**. After **[insert time period]**, the information will be automatically purged in accordance with purging

[11] For further information about these processes, see *Recommendations for First Amendment-Protected Events for State and Local Law Enforcement Agencies* at 22–23, Global Justice Information Sharing Initiative, https://it.ojp.gov/GIST/35/Recommendations-for-First-Amendment-Protected-Events-for-State-and-Local-Law-Enforcement-Agencies.

protocols (i.e., permanently removed from the repository). Refer to section K. Security and Maintenance, item 9, regarding face recognition information stored in audit logs.

Option 2: The entity has authorized access to and can perform face recognition searches utilizing image repositories not owned by the entity.

Images accessed by the **[name of entity]** for face recognition searches, in accordance with section E.1, are not maintained or owned by the **[name of entity]** and are subject to the retention policies of the respective agencies authorized to maintain those images.

Option 3: The entity is authorized to request that face recognition searches be performed by an external entity that operates a face recognition program.

The **[name of entity]** is authorized to submit face recognition search requests, in accordance with section E.1, to external agencies that own and maintain face image repositories. The images searched are subject to the retention policies of the respective agencies that maintain or own the face image repositories.

Once a face recognition image is downloaded by **[name of entity]** personnel and incorporated into a criminal intelligence record or an investigative case file, the face recognition information is then considered criminal intelligence or investigative information, and the laws, regulations, and policies applicable to that type of information or criminal intelligence govern its use.

Any images that do not originate with the **[name of entity]** will remain in the custody and control of the originating agency and will not otherwise be transferred to any other entity without authorization from the originating agency.

If the face recognition image has become or there is reason to believe that it will become evidence, including Rosario material or evidence that tends to inculpate or exculpate a suspect, in a specific criminal or other law enforcement investigation or action, the following provisions apply:

a. In those circumstances in which an image is identified as being Rosario material or having evidentiary value, the face recognition **[insert administrator or other title]** or designee will review the facts of the specific case and determine whether the image should be retained beyond the established retention period. If it is determined that it is reasonable to believe the image is Rosario material or has evidentiary value, the face recognition **[insert administrator or other title]** will authorize the transfer of the applicable image from the image repository to **[insert appropriate response; for example, "the entity's investigative case file," "the entity's case management system," or "a form of digital storage media (CD, DVD, etc.) or other portable storage device"]** and will purge the image from the repository.
b. Agencies requiring images be retained by the **[name of entity]** beyond the established retention period may make a formal, written request to the **[name of entity]** to extend retention. Each request must specify the need for extended retention, the circumstances surrounding the request, the requesting agency's case number, and a specific point of contact within the requesting agency. The **[name of entity]** reserves the right to grant or deny agency requests based on the information provided.

The **[name of entity]** retains the right to remove images from the repository earlier than the retention period, based on the limitations of information storage requirements and subject to any applicable record retention laws and statutory disclosure mandates. Early removal, however, will not be used as a means for intentionally interfering with a lawful complaint or a public records request. The retention period may be modified at any time by the **[name of entity]**, subject to applicable legal requirements.

2. **What is the entity's retention policy for probe images?**

   Probe images are not enrolled (stored) in the image repository. Retention of probe images will be the same as for the type of file (criminal case file, criminal intelligence file), whether paper or electronic, in which the information is stored.

3. **Does the entity store unidentified images in an unsolved image file?**

   Note: If the entity does not store images in an unsolved image file, then this provision would not apply. If the entity is going to maintain an unsolved image file, there must be a legal standard and retention period.

   A lawfully obtained probe image of an unknown suspect *may* be added to an unsolved image file pursuant to an authorized criminal investigation. Images in an unsolved image file are periodically compared with those in an image repository (of known persons). If a most likely candidate meets a minimum threshold of computer-evaluated similarity results, the contributor of the probe image is notified and requested to validate the continued need to store the image or determine whether the image can be purged. If, in accordance with this policy, the contributor has not validated the need to retain the image in the unsolved file, the image will be purged.

4. **Does the entity store the results—or generated list of the most likely candidates—of a face recognition search?**

   The list of most likely candidate images is not enrolled (stored) in the image repository. For **[name of entity]** investigations, the case agent will maintain the list of most likely candidates from a face recognition search within the case file.

5. **Are probe images or the results of a face recognition search retained in an audit log?**

   Probe images and face recognition search results are saved within the entity's system audit log for audit purposes only. The audit log is available only to the **[insert position, such as a face recognition administrator]** and will be purged within **[insert time period]**. The audit log is not searchable and face recognition searches cannot be performed using the audit log.

M. Accountability and Enforcement

M.1 Transparency

1. **Is the entity's face recognition policy available to the public?**

   The **[name of entity]** will be open with the public with regard to face recognition information collection, receipt, access, use, dissemination, retention, and purging practices. The **[name of entity]**'s face recognition policy will be made available in printed copy upon request and posted prominently on the **[name of entity]**'s website **[or web page]** at **[insert web address]**.

2. **Does the entity have a point of contact for handling inquiries or complaints?**

   The **[name of entity]**'s **[Privacy Officer, Face Recognition Administrator, or other position title]** will be responsible for receiving and responding to inquiries and complaints about the entity's use of the face recognition system, as well as complaints regarding incorrect information or P/CRCL protections in the image repository maintained and face recognition system accessed by the **[name of entity]**. The **[Privacy Officer, Face Recognition Administrator, or other position title]** may be contacted at **[insert mailing address or e-mail address]**.

M.2 Accountability

1. **What procedures and practices does the entity follow to enable evaluation of user compliance with system requirements, the entity's face recognition policy, and applicable law?**

   The **[name of entity]** will adopt and follow procedures and practices by which it can ensure and evaluate the compliance of users with the face recognition system requirements and with the provisions of this policy and applicable law. This will include logging access to face recognition information, may include any type of medium or technology (e.g., physical servers, virtual machines, and mobile devices) used in a work-related activity, and will entail periodic random auditing of these systems so as not to establish a discernable pattern that may influence users' actions. These audits will be mandated at least **[insert quarterly, semiannually, annually, or other time period]**, and a record of the audits will be maintained by the **[Privacy Officer, Face Recognition Administrator, or title of designee]** of the **[name of entity]** pursuant to the retention policy. Audits may be completed by an independent third party or a designated representative of the **[name of entity]**.

   Appropriate elements of this audit process and key audit outcomes will be compiled into a report and may be provided to command staff and oversight entities or governance boards.[12]

   [Entities may also release a summary of findings to the public, pursuant to law or as a matter of discretion. If so, entities should consider the optional language below.]

   Optional: The **[name of entity]** will provide an overview of audit findings to the public to enhance transparency with respect to P/CRCL protections built into the **[name of entity]**'s operations.

   Note: Statistical data may be incorporated into the publication, but the entity should be mindful of operational considerations. Actual audit logs, statistical data, or summary findings may contain PII. No PII should be included in the summary of audit findings released to the public.

2. **Does the entity have a mechanism for users or other personnel to report errors, malfunctions, or deficiencies of face recognition information and suspected or confirmed violations of face recognition policies?**

   The **[name of entity]**'s personnel or other authorized users shall report errors, malfunctions, or deficiencies of face recognition information and suspected or confirmed violations of the **[name of entity]**'s face recognition policy to the **[name of entity]**'s **[insert title of Face Recognition Administrator]**.

3. **How often does the entity review and update the provisions contained within this face recognition policy (for example, annually)?**

   The **[Privacy Officer, Face Recognition Administrator, or other position title]** will review and update the provisions contained in this face recognition policy annually and will make appropriate changes in response to changes in applicable law, technology, and/or the purpose and use of the face recognition system; the audit review; and public expectations.

[12] *Privacy, Civil Rights, and Civil Liberties Audit Guidance for the State, Local, Tribal, and Territorial Intelligence Component*, Global Justice Information Sharing Initiative, https://it.ojp.gov/GIST/181/Privacy--Civil-Rights--and-Civil-Liberties-Audit-Guidance-for-the-State--Local--Tribal--and-Territorial-Intelligence-Component.

M.3 Enforcement

1. **What is the entity's procedure for enforcement if entity personnel, a <u>participating agency</u>, or an authorized user is suspected of being or has been found to be in noncompliance with the provisions of this policy?**

   If **[name of entity]** personnel, a participating agency, or an authorized user is found to be in noncompliance with the provisions of this policy regarding the collection, receipt, access, use, dissemination, retention, and purging, the **[title of entity director]** of the **[name of entity]** will:
   - Suspend or discontinue access to information by the **[name of entity]** entity personnel, the participating agency, or the authorized user.
   - Apply appropriate disciplinary or administrative actions or sanctions.
   - Refer the matter to appropriate authorities for criminal prosecution, as necessary, to effectuate the purposes of the policy.

2. **What is the entity's policy with regard to the qualifications and number of <u>participating agency</u> personnel authorized to access the entity's <u>face recognition system</u>, and what additional sanctions are available for violations of the entity's face recognition policy?**

   The **[name of entity]** reserves the right to establish the qualifications and number of personnel having access to the **[name of entity]**'s face recognition system and to suspend or withhold service and deny access to any participating agency or participating agency personnel violating this face recognition policy.

N. Training

1. **Which personnel are required to participate in training programs before authorized access to the entity's <u>face recognition system</u>?**

   Before access to the **[name of entity]**'s face recognition system is authorized, the **[name of entity]** will require the following individuals to participate in training regarding implementation of and adherence to this face recognition policy:
   - All authorized **[name of entity]** personnel, including examiners
   - All authorized participating agency personnel
   - All authorized personnel providing information technology services to the **[name of entity]**

2. **What is covered by the entity's face recognition training program (for example, purpose of the face recognition policy, substance and intent of the provisions of the face recognition policy, impact of infractions, and possible penalties for violations)?**

   The **[name of entity]**'s face recognition policy training program will cover both:

   a. Elements of the operation of the face recognition program, including:
      - Purpose and provisions of the face recognition policy.
      - Substance and intent of the provisions of this face recognition policy and any revisions thereto relating to collection, receipt, access, use, dissemination, retention, and purging of the **[name of entity]**'s face recognition information.
      - Policies and procedures that mitigate the risk of profiling.
      - How to implement the face recognition policy in the day-to-day work of the user, whether a paper or systems user.
      - Security awareness training.
      - How to identify, report, and respond to a suspected or confirmed breach.
      - Cultural awareness training, including:

   b. Elements related to the results generated by the face recognition system
      - Originating and participating agency responsibilities and obligations under applicable federal, state, or local law and policy.

- The P/CRCL protections on the use of the technology and the information collected or received, including constitutional protections, and applicable state, local, and federal laws.
- Face recognition system functions, limitations, and interpretation of results.
- Mechanisms for reporting violations of **[name of entity]** face recognition policy provisions.
- The nature and possible penalties for face recognition policy violations, including possible transfer, dismissal, criminal liability, and immunity, if any.

3. **What specialized training does the entity require face recognition examiners to complete prior to performing comparisons and analysis of face recognition probe and candidate images?**

   In addition to the training described in M.2, the **[name of entity]** face recognition examiners are required to complete advanced specialized training to include:
   - Face recognition system functions, limitations, and interpretation of results.
   - Use of image enhancement **[if applicable, "and video editing software"].**
   - Appropriate procedures and how to assess image quality and suitability for face recognition searches.
   - Proper procedures and evaluation criteria for one-to-many and one-to-one face image comparisons.
   - Candidate image verification process.

4. **Does the entity require that investigators (those requesting the entity perform face recognition searches) complete training before they are permitted to make face recognition search requests?**

   Investigators from outside agencies are permitted to request face recognition searches from the **[name of entity]** only if prior to making requests the outside agency **[select applicable entity requirement(s) from the following list or insert the entity's established requirements:**
   - **There is a formalized agreement (e.g., a memorandum of understanding or an interagency agreement) between the [name of entity] and the outside agency, and the agreement acknowledges that requesting investigators have an understanding of the following concepts.**
   - **The outside agency first provides examples of its applicable policies (e.g., privacy) and acknowledges in writing that its requesting investigators have an understanding of the following concepts.**
   - **There is a law enforcement agency that is making the request based on a valid law enforcement purpose that falls within the authorized uses listed in section A. Purpose Statement, item 3. And the requestor provides a case number and contact information (requestor's name, requestor's agency, address, and phone number), and acknowledges an agreement with the following statement:**

     The result of a face recognition search is provided by the [name of entity] only as an investigative lead and IS NOT TO BE CONSIDERED A POSITIVE IDENTIFICATION OF ANY SUBJECT. Any possible connection or involvement of any subject to the investigation must be determined through further investigation and investigative resources.

   - **The agency completes the [name of entity]'s training on the following concepts:**
     - **Originating and participating agency responsibilities and obligations under applicable federal, state, or local law and policy.**
     - **P/CRCL protections on the use of the technology and the information collected or received.**
     - **Conditions and criteria under which the face recognition searches may be requested.**
     - **Face recognition system functions, limitations, and interpretation of results.**
     - **Use of face recognition search results as investigative leads only.**
     - **Mechanisms for reporting violations of [name of entity] face recognition policy provisions.**
     - **The nature and possible penalties for face recognition policy violations, including dismissal, criminal liability, and immunity, if any.**
     - **Operational policies.]**

5. **What training does the entity require field personnel—who are authorized to run mobile searches—to complete prior to utilizing mobile face recognition search capabilities?**

   In addition to the training described in N.2, the **[name of entity]** requires all personnel who are authorized to run a mobile search to be trained in the following areas prior to utilizing mobile face recognition search capabilities:
   - The proper and lawful use of face images for face recognition purposes.
   - How to capture high quality face images in the field for most accurate results.
   - The rules and procedures for obtaining an individual's consent to having their image captured.
   - The appropriate use and sharing of information obtained from a face recognition search.
   - The deletion of field-acquired probe images.

   Personnel who have not received this training shall not utilize mobile face recognition search capabilities.

(This Page Intentionally Left Blank)

Appendix A—Glossary of Terms and Definitions

The following is a list of terms and definitions used within the policy or provided for the purpose of enhancing the reader's understanding of the topics discussed.

Access—Information access is being able to get to particular information on a computer (usually requiring permission to use). Web access means having a connection to the internet through an access provider or an online service provider.

Access Control—The mechanisms for limiting access to certain information, based on a user's identity and membership in various predefined groups. Access control can be mandatory, discretionary, or role- or user-based.

Acquisition—The means by which an entity obtains face recognition information through the exercise of its authorities.

Agency—See Participating Agency.

Algorithm—An algorithm is a procedure or formula for solving a problem, based on conducting a sequence of specified actions. A computer program can be viewed as an elaborate algorithm. Algorithms can perform calculation, data processing, and automated reasoning tasks and are widely used throughout all areas of information technology.

Analysis—Refer to Image Analysis.

Attributes—Physical characteristics, such as gender, race, age, hair color, etc. that can be applied to a face recognition search.

Audit Trail—A generic term for recording (logging) a sequence of activities. In computer and network contexts, an audit trail tracks the sequence of activities on a system, such as user log-ins and log-outs. More expansive audit trail mechanisms would record each user's activity in detail, such as what commands were issued to the system, what records and files were accessed or modified, etc.

Audit trails are a fundamental part of computer security and used to trace (albeit usually retrospectively) unauthorized users and uses. They can also be used to assist with information recovery in the event of a system failure.

Authentication—The process of validating the credentials of a person, computer process, or device. Authentication requires that the person, process, or device making the request provides a credential that proves it is what or who it says it is. Common forms of credentials are digital certificates, digital signatures, smart cards, biometrics data, and a combination of user names and passwords. See Biometrics.

Authorization—The process of granting a person, a computer process, or device with access to certain information, services, or functionality. Authorization is derived from the identity of the person, a computer process, or a device requesting access that is verified through authentication. See Authentication.

Automated Face Recognition (AFR)—Automated face recognition (AFR) software compares patterns within the field of computer vision. Such approaches do not rely upon intrinsic models of what a face is, how it should appear, or what it may represent. In other words, the matching is not based on biological or anatomical models of what a face–or the features that make up a face—look like. Instead, the algorithm

performance is entirely dependent upon the patterns which the algorithm developer finds to be most useful for finding similarities. The patterns used in AFR algorithms do not correlate to obvious anatomical features such as the eyes, nose or mouth in a one-to-one manner, although they are affected by these features.

Biometric Template—A biometric template is a set of biometric measurement data [or features] prepared by a face recognition system from a face image.[13] The prepared set can be compared to a probe image. An enrolled image, on its own, is not a biometric template. See Features.

Biometrics—A general term used alternatively to describe (1) a characteristic or (2) a process—(1) a measureable biological (anatomical and physiological) and behavioral characteristic that can be used for automated recognition or (2) automated methods of recognizing an individual based on measureable biological (anatomical and physiological) and behavioral characteristics.[14]

Candidates—See Candidate Images.

Candidate Images—The possible results of a face recognition search. When face recognition software compares a probe image against the images contained in a repository (See Repository.), the result is a list of most likely candidate images that were determined by the software to be sufficiently similar to or most likely resemble the probe image to warrant further analysis. A candidate image is an investigative lead only and does not establish probable cause to obtain an arrest warrant without further investigation.

Candidate List—One or more most likely candidate images resulting from a face recognition search. See Candidate Images.

Center—See Fusion Center.

Civil Liberties—According to the U.S. Department of Justice's Global Justice Information Sharing Initiative, the term "civil liberties" refers to fundamental individual rights, such as freedom of speech, press, or religion; due process of law; and other limitations on the power of the government to restrain or dictate the actions of individuals.[15] They are the freedoms that are guaranteed by the Bill of Rights—the first 10 amendments to the Constitution of the United States. Civil liberties offer protection to individuals from improper government action and arbitrary governmental interference.

Civil Rights—The term "civil rights" refers to those rights and privileges of equal protection that government entities must afford to all individuals in the United States regardless of race, ethnicity, gender, national origin, religion, sexual orientation, gender identity, or other characteristics unrelated to the worth of the individual. Protection of civil rights means that government entities will take action to ensure that individuals are not discriminated against on the basis of any federal- or state- protected characteristic. For example, a state may have constitutional or statutory language regarding parental status. Generally, the term "civil rights" involves positive (or affirmative) government action to protect against infringement, while the term "civil liberties" involves restrictions on government.[16]

Collect—For purposes of this document, "gather" and "collect" mean the same thing.

Comparison—The observation of two or more faces to determine the existence of discrepancies, dissimilarities, or similarities.[17] See Face Comparison.

Computer Security—The protection of information technology assets through the use of technology, processes, and training.

Confidentiality—Refers to the obligations of individuals and institutions to appropriately use information and data under their control once they have been disclosed to them and in accordance with applicable data security laws and policies. See Privacy.

Consent—In general use, consent means compliance in or approval of what is done or proposed by another; specifically, the voluntary agreement or acquiescence by a person of age or with requisite mental capacity who is not under duress or coercion and usually who has knowledge or understanding. Related to mobile face recognition, consent means an individual agrees

[13] Glossary, FISWG, Version 1.1, February 2, 2012, https://www.fiswg.org/FISWG_Glossary_v1.1_2012_02_02.pdf.
[14] Ibid.
[15] *Civil Rights and Civil Liberties Protections Guidance*, at 4 (August 2008), https://www.dni.gov/files/ISE/documents/DocumentLibrary/Privacy/CR-CL_Guidance_08112008.pdf.
[16] The definition of "civil rights" is a modified version of the definition contained in the *National Criminal Intelligence Sharing Plan* (NCISP), at pp. 5–6. *Civil Rights and Civil Liberties Protections Guidance* (August 2008), https://www.dni.gov/files/ISE/documents/DocumentLibrary/Privacy/CR-CL_Guidance_08112008.pdf.
[17] Glossary, FISWG, Version 1.1, February 2, 2012, https://www.fiswg.org/FISWG_Glossary_v1.1_2012_02_02.pdf.

to have his or her image taken by a law enforcement officer for purposes of identification. See Revocation.

Continuous Monitoring—A system security process that comprises ongoing situational awareness of information security, vulnerabilities, threats, and incidents for each user level to support entity risk management decisions.

Credentials—Information that includes identification and proof of identification that are used to gain access to local and network resources. Examples of credentials are usernames, passwords, smart cards, and certificates.

Criminal Activity—A behavior, an action, or an omission that is punishable by criminal law.

Criminal Case Support—Administrative or analytic activities that provide relevant information to law enforcement personnel regarding the investigation of specific criminal activities or trends or specific subject(s) of criminal investigations.

Criminal Intelligence Information—Information deemed relevant to the identification of and the criminal activity engaged in by an individual who or organization that is reasonably suspected of involvement in criminal activity. Criminal intelligence records are maintained in a criminal intelligence system per 28 CFR Part 23.

Data—Inert symbols, signs, descriptions, or measures; elements of information.

Data Breach—The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses personally identifiable information (PII) or (2) an authorized user accesses or potentially accesses PII for a purpose other than authorized purposes. An entity's response to a data breach may be addressed in state law or agency policy. This may include incidents such as:

- Theft or loss of digital media—including computer tapes, hard drives, or laptop computers containing such media—upon which such information is stored unencrypted.
- Posting such information on the internet.
- Unauthorized employee access to certain information.
- Moving information to a computer otherwise accessible from the internet without proper information security precautions.
- Intentional or unintentional transfer of information to a system that is not completely open but is not appropriately or formally accredited for security at the approved level, such as unencrypted e-mail.
- Transfer of information to the information systems of a possibly hostile agency or environment where it may be exposed to more intensive decryption techniques.

Data Protection—Encompasses the range of legal, regulatory, and institutional mechanisms that guide the collection, receipt, use, dissemination, retention, purging, and protection of information.

Data Quality—Refers to various aspects of the information, such as the accuracy and validity of the actual values of the data, information structure, and database/information repository design. Traditionally, the basic elements of data quality have been identified as accuracy, completeness, currency, reliability, and context/meaning. Today, data quality is being more fully described in multidimensional models, expanding conventional views of the topic to include considerations of accessibility, security, and privacy. This concept is also addressed as one of the Fair Information Practice Principles (FIPPs), Data Quality/Integrity. See Appendix B for a full set of FIPPs.

Direct Face Recognition Collection—The entity is owner of the face recognition equipment that captures face recognition information.

Disclosure—The release, transfer, provision of access to, sharing, publication, or divulging of PII in any manner—electronic, verbal, or in writing—to an individual, agency, or organization outside the agency that collected it. Disclosure is an aspect of privacy, focusing on information which may be available only to certain people for certain purposes but which is not available to everyone.

Dissemination—See Disclosure.

Electronically Maintained—Information stored by a computer or on any electronic medium from which the information may be retrieved by a computer, such as electronic memory chips, magnetic tape, magnetic disk, compact disc optical media, or cloud technologies.

Electronically Transmitted—Information exchanged with a computer using electronic media, such as movement of information from one location to another by magnetic or optical media, or transmission over the internet, intranet, extranet, leased lines, dial-up lines, private networks, telephone voice response, or faxback systems. It does not include faxes, telephone calls, video teleconferencing, or messages left on voicemail.

Enhancement—Image enhancement is the process of adjusting digital images so that the results are more suitable for display or further image analysis. For example, removing noise, sharpening or brightening an image may make it easier to identify key features.

Enroll—The process of storing and maintaining information. Specifically in the face recognition context, biometric enrollment is capturing a face image, creating a biometric template from the image, and entering the template into a face recognition repository.[18] See Biometric Template and Repository.

Enrolled Image—An image that is loaded to, and may be stored in, an image repository (see Repository) and used as a reference image for face recognition comparisons (searches). Enrolled images do not include probe images. Some images of individuals may not be enrolled because they do not meet established criteria.

Enrollment—See Enroll.

Entity—The **[name of entity],** which is the subject and owner of the face recognition policy.

Evaluation—Refer to Image Evaluation.

Examiner—An individual who has received advanced training in the face recognition system and its features. Examiners have at least a working knowledge of the limitations of face recognition and the ability to use image editing software. They are qualified to assess image quality and appropriateness for face recognition searches and to perform one-to-many and one-to-one face image comparisons.

Examiners determine if probe images are suitable for face recognition searches, and may enhance images for the purpose of conducting a face recognition search. Though enhancements to the probe image are permissible, the examiner does not base any conclusions on a comparison between an enhanced probe image and a potential candidate photo. Examiners shall evaluate search results by comparing the original unknown probe image with the potential candidate photo.

Expression—Facial aspects resulting from muscle movement or position.[19]

Face Comparison—The manual examination of the differences and similarities between two face images or a live subject and a face image (one-to-one) for the purpose of determining if they represent the same or different persons.[20] See Face Recognition, One-to-One Face Image Comparison, and Verification.

Face Detection—Automated determination of the locations and sizes of human faces in digital images.[21]

Face Examiner—See Examiner.

Face Recognition—The automated searching for a reference image in an image repository (see Repository) by comparing the facial features of a probe image with the features of images contained in an image repository (one-to-many search). A face recognition search will typically result in one or more most likely candidates—or candidate images—ranked by computer-evaluated similarity or will return a negative result. See Candidate Images.

Face Recognition Program—An entity's face recognition initiative that includes the management of human components (management, analysts, examiners, authorized users), ownership and management of the face recognition system (technical components), and the establishment and enforcement of entity-wide processes, policies, and procedures. See Face Recognition System.

Face Recognition Software/Technology—Third-party software that uses specific proprietary algorithms to compare facial features from one specific picture—a probe image—to many others (one-to-many) that are stored in an image repository (see Repository) to determine most likely candidates for further investigation. See Candidate Images.

Face Recognition System—The technical components of a face recognition program, such as hardware, software, interfaces, image repositories, biometric templates, autogenerated candidate lists, etc. While some entities own such a system, others may only have authorized access to another entity's face recognition system. See Face Recognition Program.

Facial Recognition—See Face Recognition.

Fair Information Practice Principles—The Fair Information Practice Principles (FIPPs) are a set of internationally recognized principles that inform information privacy policies both within government and the private sector. Although specific articulations of FIPPs vary and have evolved since their genesis in the 1970s, core elements are consistent among nations, states, and economic sectors. These core elements are incorporated into information privacy

[18] Ibid.
[19] Ibid.
[20] Ibid.
[21] Ibid.

laws, policies, and governance documents around the world. They provide a straightforward description of underlying privacy and information exchange principles and a simple framework for the legal use that needs to be done with regard to privacy in integrated justice systems. Because of operational necessity, it may not always be possible to apply all of the principles equally. For example, the Individual Participation Principle (#8) may be of limited applicability in intelligence operations, as entities do not generally engage with individuals and under federal law, the Privacy Act of 1974 contains exemptions in the law enforcement context. That said, law enforcement entities and all other integrated justice systems should endeavor to apply FIPPs where practicable and ensure compliance with applicable law.

The eight principles are:
1. Purpose Specification
2. Data Quality/Integrity (See definition.)
3. Collection Limitation/Data Minimization
4. Use Limitation
5. Security Safeguards (See definition.)
6. Accountability/Audit
7. Openness/Transparency
8. Individual Participation

See Appendix B for one description of how the U.S. Department of Homeland Security applies these principles.

Features—Observable class or individual characteristics. The components of biometric templates. [22]

Filtering—In the face recognition context, filtering uses relevant physical facial attributes such as eye color, nose shape, eyebrow position, hairline, and other attributes to compare, select, and narrow results. See Attributes.

Firewall—A security solution that segregates one portion of a network from another portion, allowing only authorized network traffic to pass through according to traffic-filtering rules.

Frontal Pose—A face image captured from directly in front of the subject with the focal plane approximately parallel to the plane of the subject's face.[23]

Fusion Center—A fusion center is a collaborative effort of two or more federal, state, local, tribal, or territorial (SLTT) government agencies that combines resources, expertise, or information with the goal of maximizing the ability of such agencies to detect, prevent, investigate, apprehend, and respond to criminal or terrorist activity.[24] State and major urban area fusion centers serve as focal points within the state and local environment for the receipt, analysis, gathering, and sharing of threat-related information between federal and SLTT government agencies and private-sector partners.

Holistic Comparison—The process of comparing faces by looking at the face as a whole and not the component parts in isolation.[25]

Identity—Within a biometric system, the collective set of biographic data, images, and biometric templates assigned to one person.[26] See Face Comparison.

Image—See Probe Image and Repository.

Image Analysis—The assessment of an image to determine suitability for comparison, including the ability to discriminate significant features.[27]

Image Enhancement—See Enhancement.

Image Evaluation—Ascertaining the value of dissimilarities and similarities between two face images, where an examiner assesses the value of the details observed during the analysis and comparison steps and reaches a conclusion.[28]

Image Repository—See Repository.

Individual Characteristics—Characteristics allowing one to differentiate between individuals having the same class of characteristics (e.g., freckles, moles, and scars).[29]

Individual Responsibility—Because a privacy notice is not self-implementing, an individual within an organization's structure must also be assigned responsibility for enacting and implementing the notice.

Individualization—The determination by an examiner that there is sufficient agreement in the quality and quantity of detail to conclude that two

[22] Ibid.
[23] Ibid.
[24] ISE-SAR Functional Standard, version 1.5.5. Source: Section 511 of the 9/11 Commission Act.
[25] Glossary, FISWG, Version 1.1, February 2, 2012, https://www.fiswg.org/FISWG_Glossary_v1.1_2012_02_02.pdf.
[26] Ibid.
[27] Ibid.
[28] Ibid.
[29] Ibid.

images depict the same person.[30] Such results are generally referred for peer and supervisory reviews and approval before any dissemination of results is made.

Information—Includes any data about people, organizations, events, incidents, or objects, regardless of the medium in which it exists. Information received by law enforcement agencies can be categorized into three general areas: general data, including investigative information; tips and leads data, including suspicious activity reports; and criminal intelligence information.

Information Protection—Encompasses the range of legal, regulatory, and institutional mechanisms that guide the collection, receipt, use, dissemination, retention, purging, and protection of information.

Information Quality (IQ)—Refer to Data Quality.

Information Sharing Environment (ISE)—In accordance with Section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), as amended, the Information Sharing Environment (ISE) is a conceptual framework composed of the policies, procedures, and technologies linking the resources (people, systems, databases, and information) of SLTT agencies, federal agencies, and the private sector to facilitate terrorism-related information sharing, access, and collaboration.

Intelligence—See Criminal Intelligence Information.

Invasion of Privacy— Intrusion on an individual's solitude or into an individual's private affairs, public disclosure of embarrassing private information, publicity that puts an individual in a false light to the public, or appropriation of an individual's name or picture for personal or commercial advantage. See also Right to Privacy.

Investigative Lead—Any information which could potentially aid in the successful resolution of an investigation, but does not imply positive identification of a subject or that the subject is guilty of a criminal act.

Known Image—The image of an individual associated with a known or claimed identity and recorded electronically or by other medium (also known as exemplars).[31] Known images are enrolled and stored in an image repository. See Repository.

Law—As used by this policy, law includes any local, state, or federal constitution, statute, ordinance, regulation, executive order, policy, or court rule, decision, or order as construed by appropriate local, state, or federal officials or agencies.

Law Enforcement (LE) Agency—An organizational unit, or subunit, of a local, state, federal, or tribal government with the principal functions of prevention, detection, and investigation of crime, apprehension of alleged offenders, and enforcement of laws. LE agencies further investigations of criminal behavior based on prior identification of specific criminal activity with a statutory ability to perform arrest functions.

Law Enforcement Information—For purposes of the ISE (see Information Sharing Environment), law enforcement information means any information obtained by or of interest to a law enforcement agency or official that is both (a) related to terrorism or the security of our homeland and (b) relevant to a law enforcement mission, including, but not limited to, information pertaining to an actual or potential criminal, civil, or administrative investigation or a foreign intelligence, counterintelligence, or counterterrorism investigation; assessment of or response to criminal threats and vulnerabilities; the existence, organization, capabilities, plans, intentions, vulnerabilities, means, methods, or activities of individuals or groups involved or suspected of involvement in criminal or unlawful conduct or assisting or associated with criminal or unlawful conduct; the existence, identification, detection, prevention, interdiction, or disruption of or response to criminal acts and violations of the law; identification, apprehension, prosecution, release, detention, adjudication, supervision, or rehabilitation of accused persons or criminal offenders; and victim/witness assistance.

Lawful Permanent Resident—A foreign national who has been granted the privilege of permanently living and working in the United States.

Least Privilege Administration—A recommended security practice in which every user is provided with only the minimum privileges needed to accomplish the tasks he or she is authorized to perform.

Logs—A necessary part of an adequate security system which ensures that information is properly tracked and that only authorized individuals are getting access to the data. See also Audit Trail.

Maintenance of Information—Applies to all forms of information storage. This includes electronic systems (for example, databases or repositories) and nonelectronic storage systems (for example, filing

[30] Ibid.

[31] Ibid.

cabinets). To meet access requirements, an organization is not required to create new systems to maintain information or to maintain information beyond a time when it no longer serves an organization's purpose.

Manual Face Examination—Comparison and evaluations of the probe image and the candidate images by a trained biometric images specialist.

Match/Matching—For the purposes of face recognition, see Candidate Images.

Morphological Comparison—The direct comparison of class and individual face characteristics without explicit measurement.[32] See Comparison and Manual Face Examination.

Need to Know—As a result of jurisdictional, organizational, or operational necessities, access to sensitive information or intelligence is necessary for the conduct of an individual's official duties as part of an organization that has a right to know the information to perform or assist in a law enforcement, homeland security, or counterterrorism activity or other lawful and authorized government activity, such as to further an investigation or meet another law enforcement requirement.

Nodal Points—Measurements of distinctive face characteristics, including, but not limited to, the distance between the eyes, width of the nose, and the depth of the eye sockets. Nodal points are extracted from the face image and are transformed through the use of algorithms into a unique file called a biometric template. See Biometric Template.

No Match—A negative result from a face recognition search in which the probe image was determined not to be sufficiently similar to or resemble any of the reference images contained in an image repository.

Non-Criminal Justice Agency—An entity or any subunit thereof that provides services primarily for purposes other than the administration of criminal justice.

One-to-Many Face Image Comparison—The process whereby a probe image from one subject is compared with the features of reference images contained in an image repository, generally resulting in a list of most likely candidate images (one-to-many). See Candidate Images.

One-to-One Face Image Comparison—The process whereby a probe image from one subject is compared with a most likely candidate image that is also from one subject (one-to-one). See Comparison, Face Comparison, and Verification.

Participating Agency—An organizational entity that is authorized to contribute images and/or biometric information to a face recognition system and/or is authorized to access or receive, request, or use face recognition information from the **[name of entity]**'s face recognition system for lawful purposes through its authorized individual users. Participating agencies adhere to conditions defined in a formal agreement (e.g., MOU or interagency agreement) between the **[name of entity]** operating the face recognition program and the participating agency.

Peer Review—An additional layer of verification of face recognition results in a face recognition search process. Examiners submit face recognition search results to other authorized and trained examiners—or peers—for an independent review and cross-verification of the probe and most likely candidate images. If verified by peer(s), this step is generally followed by a supervisor's review and approval prior to dissemination. Refer to Verification.

Permissions—Authorization to perform operations associated with a specific shared resource, such as a file, a directory, or a printer. Permissions must be granted by the system administrator to individual user accounts or administrative groups.

Personally Identifiable Information (PII)—
Information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information, that is linked or linkable to a specific individual." [33]

Pose—The orientation of the face with respect to the camera, consisting of pitch, roll, and yaw. Common poses are frontal and profile.[34]

Privacy—Refers to individuals' interests in preventing the inappropriate collection, use, and release of PII. Privacy interests include privacy of personal behavior, privacy of personal communications, and privacy of personal data. Other definitions of privacy include the

[32] Ibid.
[33] For further information about the breadth of PII and how to perform an assessment of the specific risk that an individual can be identified using the information, see Revision of Office of Management and Budget Circular A-130: Managing Information as a Strategic Resource, July 2016, https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2017/m-17-12_0.pdf.
[34] Ibid.

capacity to be physically left alone (solitude); to be free from physical interference, threat, or unwanted touching (assault, battery); and to avoid being seen or overheard in particular contexts.

Privacy Policy—Short term for a privacy, civil rights, and civil liberties (P/CRCL) policy which is a printed, published statement that articulates the policy position of an organization on how it handles the PII that it gathers or receives and uses in the normal course of business. The policy should include information relating to the processes of information collection, receipt, access, use, dissemination, retention, and purging. It is likely to be informed by the FIPPs. The purpose of the P/CRCL policy is to articulate that the entity will adhere to those legal requirements and entity policy determinations that enable collection, receipt, access, use, dissemination, retention, and purging of information to occur in a manner that protects personal privacy interests. A well-developed P/CRCL policy uses justice entity resources wisely and effectively; protects the entity, the individual, and the public; and promotes public trust.

Probe Image—Any face image used by face recognition software for comparison with the face images contained within a face image repository. See Repository.

A front-facing image of an individual lawfully obtained pursuant to an authorized criminal investigation. Examples of probe images include:

- Face images captured from closed circuit TV cameras
- Face images captured from an ATM camera
- Face images provided by a victim or witness of a crime
- Face images gained from evidence (fraudulent bank card or photograph ID)
- Face sketches (for example, police artist drawings)

Protected Information—For the nonintelligence community, protected information is information about United States citizens and lawful permanent residents that is subject to information privacy or other legal protections under the Constitution and laws of the United States.

For the (federal) intelligence community, protected information includes information about "United States persons" as defined in Executive Order 12333. Protected information may also include other information that the U.S. government expressly determines by Executive Order, international agreement, policy, or other similar instrument.

For state, local, tribal, and territorial governments, protected information may include information about individuals and organizations that is subject to information privacy or other legal protections by law, including the U.S. Constitution; applicable federal statutes and regulations, such as civil rights laws and 28 CFR Part 23; applicable state and tribal constitutions; and applicable state, local, tribal, and territorial laws, ordinances, and codes. Protection may be extended to other individuals and organizations by a law enforcement entity or other state, local, tribal, or territorial agency policy or regulation.

Public—Includes:

- Any individual and any for-profit or nonprofit entity, organization, or association.
- Any governmental entity for which there is no existing specific law authorizing access to the entity's information.
- Media organizations.
- Entities that seek, receive, or disseminate information for whatever reason, regardless of whether it is done with the intent of making a profit and without distinction as to the nature or intent of those requesting information from the entity or participating entity.

Public does not include:

- Any employees of the entity or participating entity.
- People or entities, private or governmental, who assist the entity in the operation of the justice information system.
- Public entities whose authority to access information collected or received and retained by the entity is specified in law.

Public Access—Relates to what information can be seen by the public; that is, information whose availability is not subject to privacy interests or rights.

Purge—A term that is commonly used to describe methods that render data unrecoverable in a storage space or destroy data in a manner that it cannot be reconstituted. There are many different strategies and techniques for data purging, which is often contrasted with data deletion (e.g., made inaccessible except to system administrators or other privileged users).

Recognition—See Face Recognition.

Record—Any item, collection, or grouping of information that includes PII and is collected, received, accessed, used, disseminated, retained, and purged by or for the collecting agency or organization.

Redress—Laws, policies, and procedures that address public agency responsibilities with regard to

access/disclosure and correction of information and the handling of complaints from persons regarding *protected information* about them which is under the entity's control and which is exempt from disclosure and not disclosed to the individual to whom the information pertains.

Protected information includes personal information about individuals that is subject to information privacy or other legal protections by law. Protection may also be extended to organizations by entity policy or state, local, tribal, or territorial law.

Relative Frequency—How often facial features or combinations thereof occur in a given population.[35]

Repository—A location where a group of images of known individuals and biometric templates are stored and managed. An image repository is searched during a face recognition search process whereby a probe image is used by face recognition software for comparison with the images (or features within images) contained in the image repository.

Request—A request received by the **[name of entity]** to utilize face recognition in support of a criminal investigation. Submissions will not contain original evidence. Images received in a request or submission will not be stored as enrolled images within the face recognition system.

Retention—See Storage.

Revocation—In general use, revocation is the act of recall or annulment. It is the reversal of an act, the recalling of a grant or privilege, or the making void of some deed previously existing. As it relates to the revocation of consent to be photographed or the individual's image captured by a law enforcement officer to perform a mobile face recognition search for purposes of identification, once consent to capture an individual's image is given, an individual may withdraw consent with an unequivocal act or statement of withdrawal. Consent may be withdrawn by statements, actions, or a combination of statements and actions. However, the revocation of consent must clearly be a statement revoking consent; an expression of impatience or dislike is not sufficient to terminate consent.

Revoke—See Revocation.

Right to Information Privacy—The right to be left alone, in the absence of some reasonable public interest in collecting, accessing, retaining, and disseminating information about an individual's activities. Invasion of the right to privacy can be the basis for a lawsuit for damages against the individual or entity violating an individual's privacy.

Right to Know—A requirement for access to specific information to perform or assist in a lawful and authorized government function. Right to know is determined by the mission and functions of a law enforcement, homeland security, counterterrorism, or other lawful and authorized government activity, or the roles and responsibilities of particular personnel in the course of their official duties.

Role-Based Access—A type of access authorization that uses roles to determine access rights and privileges. A role is a symbolic category of users that share the same security privilege.

Search—For the purposes of face recognition, the act of comparing a probe image against an image repository.[36] See Repository.

Search Filters—See Filtering.

Search Result Set—The candidate list returned from a face recognition search.[37] See Candidate Images.

Security—Refers to the range of administrative, technical, and physical business practices and mechanisms that aim to preserve privacy and confidentiality by restricting information access to authorized users for authorized purposes. Computer and communications security efforts also have the goal of ensuring the accuracy and timely availability of information for the legitimate user set, as well as promoting failure resistance in the electronic systems overall. Security safeguarding of information is a Fair Information Practice Principle (FIPP). See Appendix B.

Source Entity—Refers to the entity or organizational entity that originates face recognition information.

Storage—In a computer, storage is the place where data is held in electromagnetic or optical form for access by a computer processor. There are two general usages:

- Storage is frequently used to mean the devices and data connected to the computer through input/output operations—that is, hard disk and tape systems and other forms of storage that do not include computer memory and other in-

[35] Glossary, FISWG, Version 1.1, February 2, 2012, https://www.fiswg.org/FISWG_Glossary_v1.1_2012_02_02.pdf.

[36] Ibid.

[37] Ibid.

computer storage. This is probably the most common meaning in the IT industry.

- In more formal usage, storage has been divided into (1) primary storage, which holds data in memory (sometimes called "random access memory," or RAM) and other built-in devices, such as the processor's L1 cache, and (2) secondary storage, which holds data on hard disks, tapes, and other devices requiring input/output operations. Primary storage is much faster to access than secondary storage because of the proximity of the storage to the processor or because of the nature of the storage devices. On the other hand, secondary storage can hold much more data than primary storage.

Submission—See Request.

System Bias—Errors repeatedly introduced through automation (e.g., errors in biometric template generation or comparison). Errors repeatedly introduced through operational practices in an organization or unit (e.g., improper lighting or camera position guidance).[38]

Template—See Biometric Template.

Uncontrolled Image—An image for which the subject did not pose (e.g., security camera images, cell phone photograph taken by a witness).

Unsolved Image File—A lawfully obtained probe image of an unknown suspect *may* be added by authorized law enforcement users to an unsolved image file pursuant to an authorized criminal investigation and if a search has produced no candidates and the subject remains unknown. Images in an unsolved image file are periodically compared with the known images in an image repository. Images enrolled in an unsolved image file should be required to be validated periodically by the contributors to ensure that the criminal investigation remains active and that the image remains relevant to the investigation.

User—An **[name of entity]** employee or an individual representing a participating agency who is authorized and trained to access and use, or receive results from, an entity's face recognition system for lawful purposes.

Valid Law Enforcement Purpose—A purpose for information/intelligence gathering, development, or collection, use, retention, or sharing that furthers the authorized functions and activities of a law enforcement agency, which may include the prevention of crime, ensuring the safety of the public, protection of public or private structures and property, furthering officer safety (including situational awareness), and homeland and national security, while adhering to law and agency policy designed to protect the P/CRCL of Americans.[39] Similar terms include "reasonable law enforcement purpose,"[40] "legitimate law enforcement purpose," and "authorized law enforcement activity."[41]

Verification—In a biometric system, the process of conducting a one-to-one comparison. A task where the face recognition system attempts to confirm an individual's claimed identity by comparing the biometric template generated from a submitted face image with a specific known template generated from a previously enrolled face image.

A review and independent analysis of the conclusion of another examiner.[42]

[38] Ibid.

[39] See *Developing a Policy on the Use of Social Media in Intelligence and Investigative Activities: Guidance and Recommendations*, Global, BJA, OJP, DOJ, February 2013, https://it.ojp.gov/GIST/132/Developing-a-Policy-on-the-Use-of-Social-Media-in-Intelligence-and-Investigative-Activities--Guidance-and-Recommendations- and also in the *Real-Time and Open Source Analysis (ROSA) Resource Guide*, Criminal Intelligence Coordinating Council (CICC), Global, BJA, OJP, DOJ, July 2017, https://it.ojp.gov/GIST/1200/Real-Time-and-Open-Source-Analysis--ROSA--Resource-Guide (using "valid law enforcement purpose").

[40] *Recommendations for First Amendment-Protected Events for State and Local Law enforcement Agencies*, CICC, Global, OJP, DOJ, and DHS, December 2011, https://it.ojp.gov/GIST/35/Recommendations-for-First-Amendment-Protected-Events-for-State-and-Local-Law-Enforcement-Agencies.

[41] The term "authorized law enforcement activity" is used, for example, in *The Attorney General's Guidelines For Domestic FBI Operations*, as provided in sections 509, 510, 533, and 534 of title 28, United States Code, and Executive Order 12333, September 29, 2008.

[42] Glossary, FISWG, Version 1.1, February 2, 2012, https://www.fiswg.org/FISWG_Glossary_v1.1_2012_02_02.pdf.

Appendix B—Fair Information Practice Principles (FIPPs)

The Fair Information Practice Principles (FIPPs) are a set of internationally recognized principles that inform information privacy policies within both government and the private sector.

Although specific articulations of FIPPs vary and have evolved since their genesis in the 1970s, core elements are consistent among nations, states, and economic sectors. These core elements are incorporated into data privacy laws, policies, and governance documents around the world. For example, FIPPs are:

- At the core of the Privacy Act of 1974, which applies these principles to U.S. federal agencies.[43]
- Internationally influential, especially as articulated by the Organisation for Economic Co-operation and Development.
- Mirrored in many states' laws and in law enforcement entities' and fusion centers' privacy policies.
- Used by numerous foreign countries and international organizations.

The following formulation of FIPPs is used and implemented for the Information Sharing Environment (ISE) by the U.S. Department of Homeland Security (DHS).[44] For a definition of the Information Sharing Environment, refer to Appendix A, Glossary of Terms and Definitions. Note, however, that under certain circumstances, FIPPs may be superseded by authorities paralleling those provided in the federal Privacy Act; state, local, tribal, or territorial law; or entity policy.

1. **Purpose Specification—**Agencies should specifically articulate the authority that permits the collection of personally identifiable information (PII). The purpose(s) for which PII is collected should be specified at the time of data collection. Subsequent use of this data should be limited to the original purpose for which the PII was collected (or other purposes *compatible* with the original collection purpose).

   Implementing the Purpose Specification Principle—Agencies are bound by specific constitutional and statutory authorities that circumscribe their ability to collect PII. The following are examples of ways agencies may implement this principle:
   - Ensure that a valid lawful purpose exists and is documented for all collection of PII.
   - Include the source and authority for the data so that access restrictions can be applied.
   - Upon receipt of data containing PII from third parties, if possible, identify the purpose for which it was collected initially and limit agency use to only those uses compatible with the original purpose supporting collection.
   - Ensure that metadata or other tags are associated with the data as it is shared.
   - Institute a two-individual review and approval process to consider any Privacy Act or other legal or policy limitation before permitting use or sharing of data for purposes other than that for which it was collected.

[43] 5 U.S.C. § 552a.
[44] 6 U.S.C. § 142.

2. **Data Quality/Integrity—**PII collected should be relevant to the purposes identified for its use and should be accurate, complete, and up to date.

   Implementing the Data Quality/Integrity Principle—One important way to minimize potential downstream privacy and civil liberties concerns is to ensure that any information collected, stored, and disseminated is accurate. This includes ensuring that the information provides sufficient context for any PII. Possible approaches include:
   - Properly labeling PII.
   - Determining a policy for safeguarding PII if there are "mixed" databases (i.e., those databases with personal information on U.S. individuals and others, regardless of nationality).
   - Instituting a source verification procedure to ensure that reporting is based only on authorized data.
   - Reconciling and updating PII whenever new relevant information is collected.
   - Developing a protocol for ensuring that data corrections are passed to those entities with which information has been shared.
   - Creating a documented process for identifying and addressing situations in which data has been erroneously received, is inaccurate, or has been expunged.

3. **Collection Limitation/Data Minimization—**PII should be collected only if the data is directly relevant and necessary to accomplish the specified purpose. PII should be obtained by lawful and fair means and retained only as long as is necessary to fulfill the specified purpose.

   Implementing the Collection Limitation/Data Minimization Principle—Collection limitation may be implemented by:
   - Designing a data storage system to pull data for review and then, if appropriate, automatically purging data after the specified retention period has been reached.
   - Limiting data field elements to only those that are relevant.
   - Ensuring that all distributed reports and products contain only that personal information that is relevant and necessary (nothing extraneous or superfluous).
   - Ensuring that all shared information with PII meets the required thresholds for sharing, such as reasonable suspicion.

4. **Use Limitation—**PII should not be disclosed, made available, or otherwise used for purposes other than those specified except (a) with the consent of the individual or (b) by authority of the law.

   Implementing the Use Limitation Principle—Sharing information should be tempered by adherence to key principles, such as "authorized access." Use limitation may be implemented by:
   - Limiting users of data to those with credential-based access.
   - Requiring that justifications be entered and logs maintained for all queries with sensitive PII and that an internal review process of those logs takes place at specified intervals.
   - Requiring senior analysts to review all reports that use PII before dissemination to ensure (a) that PII is relevant and necessary and (b) that the recipient is authorized to receive the information in the performance of an authorized activity.
   - Prior to sharing information, verify that partners have a lawful purpose for requesting information.
   - Creating multiple use-based distribution lists and restricting distribution to those authorized to receive the information.

5. **Security/Safeguards—**Agencies should institute reasonable security safeguards to protect PII against loss, unauthorized access, destruction, misuse, modification, or disclosure.

   Implementing the Security/Safeguards Principle—This principle can be implemented by:
   - Maintaining up-to-date technology for network security.
   - Ensuring that access to data systems requires that users meet certain training and/or vetting standards and that such access is documented and auditable.
   - Ensuring that physical security measures are in place, such as requiring an identification card, credentials, and/or passcode for data access; disabling computers' USB ports; and implementing firewalls to prevent access to commercial e-mail or messaging services.
   - Implementing a protocol with technical and manual safeguards to ensure the accuracy and completeness of data system purges when records are deleted at the end of their retention period.

- Ensuring that data system purge protocols include complete record deletion on all backup systems.
- Transitioning older repositories into more modern systems to improve access controls.
- Masking data so that it is viewable only to authorized users.
- Maintaining an audit log to record when information is accessed and by whom for review by senior staff at specified intervals.
- Requiring authorized users to sign nondisclosure agreements.

6. **Accountability/Audit—**Agency personnel and contractors are accountable for complying with measures implementing FIPPs, for providing training to all employees and contractors who use PII, and for auditing the actual use and storage of PII.

   Implementing the Accountability/Audit Principle—Strong policies must not only be in place but also be effectively implemented. Accountability can be demonstrated by:
   - Ensuring that upon entry for duty, all staff members take an oath to adhere to the privacy and civil liberties protections articulated in the entity's or host agency's mission, core values statements, other key documents, and/or the U.S. Constitution.
   - Conducting effective orientation and periodic refresher training, including privacy, civil rights, and civil liberties (P/CRCL) protections, for all individuals handling PII.
   - Tailoring training to specific job functions, database access, or data source/storage requirements.
   - Conducting regular audits of all systems in which records are kept to ensure compliance with P/CRCL policies and all legal requirements.
   - Following a privacy incident, establishing a handling procedure for any data breaches or policy violations.
   - Denying database access to individuals until they have completed mandatory systems access training (including training for handling of PII), show a mission need for access, and have any necessary clearances.
   - Developing targeted and consistent corrective actions whenever noncompliance is found.

7. **Openness/Transparency—**To the extent feasible, agencies should be open about developments, practices, and policies with respect to the collection, use, dissemination, and maintenance of PII. Agencies should publish information about policies in this area, including the P/CRCL policy, and contact information for data corrections and complaints.

   Implementing the Openness/Transparency Principle—Agencies can implement the Openness/Transparency principle by:
   - Providing reports to an internal or external oversight body concerned with P/CRCL issues, including P/CRCL audit results.
   - Publishing the P/CRCL policy and redress procedures.
   - Meeting with community groups through initiatives or other opportunities to explain the agency's mission and P/CRCL protections.
   - Responding in the fullest way possible to freedom of information and/or sunshine requests and fully explaining any denial of information requests from the public.
   - Conducting and publishing Privacy Impact Assessments and Privacy Impact Analysis in advance of implementing any new technologies that affect PII, thereby demonstrating that P/CRCL issues have been considered and addressed.

8. **Individual Participation—**To the extent practicable, involve the individual in the process of using PII and seek individual consent for the collection, use, dissemination, and maintenance of PII. Agencies should also provide mechanisms for appropriate access, correction, and redress regarding the agency's use of PII.

   Implementing the Individual Participation Principle—To the extent appropriate, agencies can implement the Individual Participation principle by:
   - Collecting information directly from the individual, to the extent possible and practical.
   - Providing the individual with the ability to find out whether an agency maintains a record relating to him or her and, if not (i.e., access and/or correction is denied), then providing the individual with notice as to why the denial was made and how to challenge such a denial.
   - Putting in place a mechanism by which an individual is able to prevent information about him or her that was obtained for one purpose from being used for other purposes without his or her knowledge.

(This Page Intentionally Left Blank)

Appendix C—Listing of Federal Laws

The U.S. Constitution is known as the primary authority that applies to federal as well as state, local, tribal, and territorial (SLTT) entities. State constitutions cannot provide a lower level of privacy and other civil liberties protection than that established by the U.S. Constitution, but states may broaden constitutional rights guaranteed by their own constitutions.

Civil liberties protections are primarily founded in the Bill of Rights. They include the basic freedoms, such as free speech, assembly, and religion; freedom from unreasonable search and seizure; due process; etc. Statutory civil rights protections in the U.S. Constitution may, in addition, directly govern state action. These include the Civil Rights Act of 1964, as amended; the Rehabilitation Act of 1973; the Equal Educational Opportunities Act of 1974; the Americans with Disabilities Act of 1990; Title VIII of the Civil Rights Act of 1968 (Fair Housing Act); the Voting Rights Act of 1965; and the Civil Rights of Institutionalized Individuals Act.

While in general, SLTT entities may not be bound directly by most statutory federal privacy and other civil liberties protection laws in the face recognition information collection sharing context, compliance may be required **indirectly** by funding conditions (e.g., Title VI of the Civil Rights Act of 1964), operation of the Commerce Clause of the U.S. Constitution, or a binding agreement between a federal agency and an SLTT entity (e.g., a memorandum of agreement or a memorandum of understanding). When relevant or possibly relevant, entities/agencies are advised to list laws, regulations, and policies within their face recognition policies, noting those that may potentially affect the sharing of information.

The development of a face recognition policy is primarily designed for entity personnel and authorized users to ensure that they are aware of the legal and privacy framework within which they and the entity must operate. If the applicability and requirements of various laws, regulations, or sharing agreements are not spelled out or referenced in an entity's face recognition policy, staff and user accountability is greatly diminished; mistakes are made; privacy violations occur; and the public's (and other agencies') confidence in the ability of the entity to protect face recognition information is compromised. When staff members know the rules through sound policy and procedure communicated through ongoing training activity, face recognition information sharing is enhanced.

Currently, U.S. federal laws do not specifically address face recognition. A few states have enacted or introduced legislation regarding biometric information. These generally fall into one of three categories regarding the collection, retention, and use of biometric information: (1) of students; (2) by businesses; and (3) by government actors. Three states—Texas,[45] Illinois,[46] and Washington[47]—have adopted laws regulating commercial use of biometric identifiers gathered through certain types of face recognition technology. Five state legislatures (as of

[45] Capture or Use of Biometric Identifier, Texas Business and Commerce Code §503.001.
[46] Biometric Information Privacy Act, 740 Illinois Compiled Statutes 14.
[47] Biometric Identifiers, Washington House Bill 1493, Chapter 299, effective July 23, 2017.

January 1, 2017)—Alaska,[48] Connecticut,[49] Massachusetts,[50] Montana,[51] and New Hampshire[52]—have also introduced bills that would regulate the collection, retention, and use of biometric data. Arizona and Missouri have pending bills regarding student privacy and limitations on the collection of student biometric data without parental consent. Finally, many state laws governing data security and breach response include biometric information in their definitions of covered personal information. For example, North Carolina's Identity Theft Protection Act lists biometric data as an element of identifying information that, in combination with a person's name, constitutes personal information. This law requires any entity conducting business in the state and maintaining personal information of a resident to take reasonable measures to protect the information against unauthorized access.[53]

As of February 2011, there is no U.S. federal law requiring that an individual identify him- or herself during a *Terry*[54] stop, but *Hiibel*[55] held that states may enact such laws, provided the law requires the officer to have reasonable and articulable suspicion of criminal involvement.[56] Twenty-four states have enacted stop and identify laws. Although the *Hiibel* case did not directly involve the deputy's use of a biometric technology, the opinion lays the foundation for state legislatures to authorize law enforcement officials to use face recognition systems. Unresolved by *Hiibel* is whether the possible loss of privacy posed by automated face recognition applications is outweighed by improved law enforcement. Nevertheless, many of the privacy issues raised by the intersection of *Hiibel* and biometric technologies can be addressed through reasonable controls over how face recognition systems are utilized in the field and how the data they capture and create will be managed.[57]

The following are synopses of primary federal laws that an entity should review and, where appropriate, consider citing in a face recognition policy to protect face recognition data and any personally identifiable information later associated with the face recognition information. As face recognition information may be incorporated as one piece of information into a larger case file, the following federal laws may be applicable. The list is arranged in alphabetical order by popular name.

1. **Applicants and Recipients of Immigration Relief Under the Violence Against Women Act of 1994 (VAWA), Public Law 103-322, September 13, 1994, and the Victims of Trafficking and Violence Prevention Act of 2000 (T and U nonimmigrant status for victims of trafficking and other serious crimes), Public Law 106-386, Oct. 28, 2000, 8 U.S.C. § 1367, Penalties for Disclosure of Information—**The governing statute prohibits the unauthorized disclosure of information about VAWA, T, and U cases to anyone other than an officer or employee of the U.S. Department of Homeland Security, the U.S. Department of Justice, the U.S. Department of State, or parties covered by exception when there is a need to know. This confidentiality provision is commonly referred to as "Section 384" because it originally became law under Section 384 of the Illegal Immigration Reform and Immigrant Responsibility Act (IIRIRA) of 1996, which protects the confidentiality of victims of domestic violence, trafficking, and other crimes who have filed for or have been granted immigration relief. 8 U.S.C. § 1367 Information is defined as any information relating to aliens who are seeking or have been approved for nonimmigrant or immigrant status as (1) battered spouses, children, or parents under provisions of VAWA; (2) victims of a severe form of human trafficking who generally are cooperating with law enforcement authorities (T nonimmigrant status); or (3) aliens who have suffered substantial physical

[48] *Introduced* Collection of Biometric Information, House Bill 72, 2017 Regular Session.
[49] *Introduced* Connecticut House Bill 5522, 2017 Regular Session.
[50] *Introduced* Massachusetts Senate Bill 750, Chapter 93H, Section 1 and 2 2017 Regular Session.
[51] *Introduced* Montana Biometric Information Privacy Act, House Bill 518, 2017 Regular Session.
[52] *Introduced* Biometric Information Privacy Act, New Hampshire House Bill 523, 2017 Regular Session.
[53] *Developing Laws Address Flourishing Commercial Use of Biometric Information,* Claypoole, Ted, and Stoll, Cameron, Business Law Today, American Bar Association, May 2016, https://www.americanbar.org/publications/blt/2016/05/08_claypoole.html.
[54] *Terry v. Ohio*, 392 U.S. 1 (1968).
[55] *Hiibel v. Sixth Judicial District Court*, 542 U.S. 177 (2004).
[56] The *Hiibel* Court held, "The principles of *Terry* permit a State to require a suspect to disclose his name in the course of a *Terry* stop."—542 U.S. at 187.
[57] *Privacy Impact Assessment Report for the Utilization of Facial Recognition Technologies to Identify Subjects in the Field,* NIets—The International Justice and Public Safety Network, June 30, 2011.

or mental abuse as the result of qualifying criminal activity and have been, are being, or are likely to be helpful in the investigation or prosecution of that activity (U nonimmigrant status). This includes information pertaining to qualifying family members who receive derivative T, U, or VAWA status. Because 8 U.S.C. § 1367 applies to any information about a protected individual, this includes records or other information that do not specifically identify the individual as an applicant for or a beneficiary of T nonimmigrant status, U nonimmigrant status, or relief under VAWA.

2. **Criminal Intelligence Systems Operating Policies, 28 CFR Part 23, Code of Federal Regulations, Title 28, Chapter 1, Part 23**—This is a guideline for law enforcement agencies that operate federally funded multijurisdictional criminal intelligence systems. The operating principles of 28 CFR Part 23 provide guidance to law enforcement regarding how to operate criminal intelligence information systems effectively while safeguarding privacy, civil rights, and civil liberties (P/CRCL) during the collection, storage, and dissemination of criminal intelligence information. The regulation governs the intelligence information systems' process, which includes information submission or collection, secure storage, inquiry and search capability, controlled dissemination, and review and purge processes.

3. **Driver's Privacy Protection Act (DPPA) of 1994, 18 U.S.C. 2721 and 2725—**18 U.S.C. 2725 (4) defines "highly restricted personal information" as **an individual's photograph or image**, social security number, medical or disability information. 18 U.S.C. 2721(b)(1) states that personal information (as described in 18 U.S.C. 2725(4), above) may be disclosed for use by any government agency, including any court or law enforcement agency, in carrying out its functions, or any private person or entity acting on behalf of a federal, state, or local agency in carrying out its functions. § 2721-2725 restricts access and prohibits the release of personal information from state motor vehicle records to ensure the privacy of persons whose records have been obtained by that department in connection with a motor vehicle record unless certain criteria are met.

4. **E-Government Act of 2002, Public Law 107–347, 208, 116 Stat. 2899 (2002)—**Office of Management and Budget (OMB) (03-22, OMB Memorandum, M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002)—OMB implementing guidance for this act requires federal agencies to perform privacy impact assessments (PIAs) for new information technologies that develop or procure new information technology involving the collection, maintenance, or dissemination of information in identifiable form or that make significant changes to existing information technology that manages information in identifiable form. A PIA is an evaluation of how information in identifiable form is collected, stored, protected, shared, and managed. The purpose of a PIA is to demonstrate that system owners and developers have incorporated P/CRCL protections throughout the entire life cycle of a system. The act requires an agency to make PIAs publicly available, except when an agency, in its discretion, determines that publication of the PIA would raise security concerns or reveal classified (i.e., national security) or sensitive information. Although this act does not apply to SLTT partners, this tool is useful for identifying and mitigating privacy risks and for notifying the public what PII the SLTT agency is collecting, why PII is being collected, and how the PII will be collected, used, accessed, shared, safeguarded, and stored.

5. **Enhanced Border Security and Visa Reform Act of 2002, H.R. 3525**—In the Enhanced Border Security and Visa Entry Reform Act of 2002, the U.S. Congress mandated the use of biometrics in U.S. visas. This law requires that U.S. embassies and consulates abroad must issue to international visitors, "only machine-readable, tamper-resistant visas and other travel and entry documents that use biometric identifiers." Additionally, the Homeland Security Council decided that the U.S. standard for biometric screening is 10 fingerprint scans collected at all U.S. embassies and consulates for visa applicants seeking to come to the United States.

6. **Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. § 1232g; 34 CFR Part 99**—FERPA governs the disclosure of students' biometric information, to the extent that it is contained in student records. A student's biometric record is included in the definition of personally identifiable information, and is a type of information that may be included in students' education records. As such, FERPA prohibits schools from releasing students' biometric information without parental consent, to the extent that it is contained

in students' education records, with some limited exceptions.[58]

7. **Federal Civil Rights laws, 42 U.S.C. § 1983, United States Code, Title 42, Chapter 21, Subchapter I, § 1983—**This is a federal statute that allows an individual to sue public officials in federal court for violations of the individual's civil rights. Civil rights include such things as the Fourth Amendment's prohibitions against unreasonable search and seizure, violations of privacy rights, and violations of the right to freedom of religion, free speech, and free association. It serves as a deterrent to unlawful collection, use, or sharing of information rather than providing specific authority or a prohibition to the collection, use, or sharing of information.

8. **Federal Records Act, 44 U.S.C. § 3301, United States Code, Title 44, Chapter 33, § 3301**—This chapter contains the laws governing disposal of records made or received by a federal agency in the normal course of business. It discusses procedures and notices, if required, and the role of the federal archivist. The law applies only to federal agencies, but there may be similar state or local laws applicable to state and local agencies.

9. **Freedom of Information Act (FOIA), 5 U.S.C. § 552, United States Code, Title 5, Part I, Chapter 5, Subchapter II, § 552—**The federal FOIA, enacted in 1966, provides access to federal agency records or information. It does not, however, allow access to state or local government records. Nearly all states have their own public access statutes that provide access to state- and local-agency records. The interaction of federal and state FOIA laws can create complex issues. Federal statutes, in essence, provide a baseline of legal protections for individuals. While state legislatures may pass laws to supplement these federal guidelines, state laws that interfere with or are contrary to a federal law are preempted. By virtue of the Supremacy Clause of the U.S. Constitution (Article VI, Clause 2), federal law may restrict access to records otherwise available pursuant to a state's FOIA by requiring that certain information be kept confidential. Thus, federal confidentiality requirements may supersede a state FOIA statute mandating public disclosure of a record, but only when there is a specific federal statute (other than the federal FOIA) that mandates the records be kept confidential. In short, records may be available under one FOIA statute but not pursuant to another.

10. **Health Insurance Portability and Accountability Act (HIPAA) of 1996, 42 U.S.C. § 201, United States Code, Title 42, Chapter 6A, Subchapter I, § 201; Public Law 104-191**—HIPAA was enacted to improve the Medicare and Medicaid programs and the efficiency and effectiveness of the nation's health care system by encouraging the development of a national health information system through the establishment of standards and requirements for the electronic transmission of health information. To that end, Congress directed the U.S. Department of Health and Human Services (HHS) to issue safeguards to protect the security and confidentiality of health information. To implement HIPAA's privacy requirements, HHS promulgated regulations setting national privacy standards for health information: the Standards for Privacy of Individually Identifiable Health Information (the "Privacy Rule")—42 U.S.C. §1320d-2; 45 CFR Parts 160, 164 (2003).

11. **HIPAA, Standards for Privacy of Individually Identifiable Health Information, 45 CFR Parts 160 and 164, Code of Federal Regulations, Title 45, Parts 160 and 164**—This "Privacy Rule" sets forth national standards for the privacy and security of individually identifiable health information (45 CFR Part 164, Subpart E (2003)). This rule has been described as providing a "federal floor" of safeguards to protect the confidentiality of medical information. State laws that provide stronger privacy protection will continue to apply over and above the federal privacy protection. The general rule under these standards states that a covered entity may not use or disclose protected health information except as permitted or required by the rules (45 CFR Part 164.502(a) and §164.103 [defining protected health information and use]). The Privacy Rule applies to the following covered entities: (1) a health plan, (2) a health care clearinghouse, and (3) a health care provider who transmits any health information in electronic form in connection with certain transactions (42 U.S.C. §1320d-1(a) (2003); 45 CFR Part 160.102 (2003). Since the Privacy Rule applies only to a covered entity, a governmental body begins its inquiry by first determining whether it is a covered entity under the Privacy Rule (45 CFR Part 160.103

[58] *Developing Laws Address Flourishing Commercial Use of Biometric Information,* Claypoole, Ted, and Stoll, Cameron, Business Law Today, American Bar Association, May 2016, https://www.americanbar.org/publications/blt/2016/05/08_claypoole.html.

(2003) [defining health plan, health care clearinghouse, health care provider]). If it is a covered entity, it then looks to the Privacy Rule for a permitted or required disclosure.

Section 164.510(b)(3) permits (but does not require) a health care provider, when a patient is not present or is unable to agree or object to a disclosure due to incapacity or emergency circumstances, to determine whether disclosing a patient's information to the patient's family, friends, or other persons involved in the patient's care, is in the best interests of the patient. Where a provider determines that such a disclosure is in the patient's best interests, the provider would be permitted to disclose only the protected health information (PHI) that is directly relevant to the person's involvement in the patient's care.

This permission clearly applies where a patient is unconscious. However, there may be additional situations in which a health care provider believes, based on professional judgment, that the patient does not have the capacity to agree or object to the sharing of PHI at a particular time and that sharing the information is in the best interests of the patient at that time. These may include circumstances in which a patient is suffering from temporary psychosis or is under the influence of drugs or alcohol.

12. **Indian Civil Rights Act of 1968, 25 U.S.C. § 1301 et seq., United States Code, Title 25, Chapter 15, Subchapter I—**This act contains definitions of relevant terms and extends certain constitutional rights to Indian tribes exercising powers of self-government.

13. **National Child Protection Act of 1993, Public Law 103-209 (December 20, 1993), 107 Stat. 2490—**In each state, an authorized criminal justice agency of the state shall report child abuse crime information to or index child abuse crime information in the national criminal history background check system. A criminal justice agency can satisfy the requirement by reporting or indexing all felony and serious misdemeanor arrests and dispositions. The U.S. Attorney General (AG) is required to publish an annual statistical summary of child abuse crimes. The act requires that 80 percent of final dispositions be entered in the state databases by December 1998, with steps being taken toward 100 percent entry.

    A 1994 amendment required that the AG—in consultation with federal, state, and local officials, including officials responsible for criminal history record systems, and representatives of public and private care organizations and health, legal, and social welfare organizations—shall develop guidelines for the adoption of appropriate safeguards by care providers and by the state for protecting children, the elderly, and individuals with disabilities from abuse.

14. **NIST Special Publication 800-53 (Appendix J) *Security and Privacy Controls for Federal Information Systems and Organizations*—**Federal agencies are required to ensure that privacy protections are incorporated into information security planning. To that end, SP 800-53 Rev. 4 features eight families of privacy controls that are based on FIPPs. The proliferation of social media, Smart Grid, mobile, and cloud computing as well as the transition from structured to unstructured information and metadata environments have added significant complexities and challenges for federal organizations in safeguarding privacy. These challenges extend well beyond the traditional information technology security view of protecting privacy, which focused primarily on ensuring confidentiality. The use of these standardized privacy controls will provide a more disciplined and structured approach for satisfying federal privacy requirements and demonstrating compliance with those requirements. Like their federal partners, SLTT agencies may use the privacy controls when evaluating their systems, processes, and programs.

15. **Preparing for and Responding to a Breach of Personally Identifiable Information, OMB Memorandum M-17-12 (January 2017)**—This Memorandum sets forth the policy for federal agencies to prepare for and respond to a breach of PII. It includes a framework for assessing and mitigating the risk of harm to individuals potentially affected by a breach, as well as guidance on whether and how to provide notification and services to those individuals. This memorandum is intended to promote consistency in the way agencies prepare for and respond to a breach by requiring common standards and processes.

16. **Privacy Act of 1974, 5 U.S.C. § 552a, United States Code, Title 5, Part I, Chapter 5, Subchapter II, § 552a—**The Privacy Act establishes a code of fair information practices that governs the collection, maintenance, use, and dissemination of information about individuals that is maintained in systems of records by federal

agencies. A system of records is a group of records under the control of an agency from which information is retrieved by the name of the individual or by some identifier assigned to the individual. The Privacy Act prohibits the disclosure of a record about an individual from a system of records without the written consent of the individual, unless the disclosure is pursuant to one of 12 statutory exceptions. The act also provides individuals with a means by which to seek access to and amendment of their records and sets agency record-keeping requirements. In addition, the Privacy Act requires that agencies give the public notice of their systems of records by publication in the *Federal Register*.

17. **Protection of Sensitive Agency Information, Office of Management and Budget Memorandum M-06-16 (June 2006)—**This memorandum provides a security checklist from the National Institute of Standards and Technology (NIST) to protect remote information removed from or accessed from outside an agency's physical location specific to personally identifiable information (PII). The NIST checklist requires that agencies verify PII in need of protection, confirm the adequacy of organization policy surrounding PII protection, and implement any necessary protections for PII transported or stored off-site or accessed remotely. In addition to the NIST checklist, the memorandum recommends implementing information encryption on all mobile devices, allowing remote access only with two-factor authentication, using timeout functions on devices, and logging all computer-readable information extracts from databases with sensitive information, while verifying that each extract has either been erased within 90 days or its use is still required.

18. **REAL ID Act of 2005, Public Law 109–13, Division B, 119 Statute 302, enacted May 11, 2005—**The REAL ID Act requires states to issue driver's licenses and identification cards that comply with standards established by the U.S. Department of Homeland Security if those identifying documents will be used to gain access to federal facilities, board federally regulated commercial aircraft, or enter nuclear power plants. Of particular note, the REAL ID Act requires that a face image be captured for each person ***applying*** for a driver's license or identification card versus existing practices in most states that only capture face images that are ultimately ***issued*** a card. While all states capture face images as part of the routine issuance process for driver's licenses and identification cards, laws in 32 states grant exceptions to the photograph requirement for individuals, including religious objectors, overseas military personnel, and persons unable to visit a service center due to physical disabilities. The REAL ID act further requires departments of motor vehicles to make reasonable efforts to ensure that an applicant does not have more than one driver's license or identification card already issued by that state under a different identity. Many states are already complying with this requirement through the use of face recognition systems. It not only requires the collection of face images but implicitly authorizes the creation of biometric templates used by face recognition systems.

19. **Section 210401 of the Violent Crime Control and Law Enforcement Act of 1994, 42 U.S.C. § 14141—**This is a federal statute that provides that it shall be unlawful for any governmental authority or its agent to engage in a pattern or practice of conduct by law enforcement officers that violates the Constitution or laws of the United States. It authorizes the Attorney General to bring civil actions to obtain injunctive or declaratory relief to eliminate the unlawful or unconstitutional pattern or practice.

20. **U.S. Constitution, First, Fourth, Fifth, Sixth, and Fourteenth Amendments—**The Bill of Rights establishes minimum standards for the protection of the civil rights and civil liberties of persons within the United States. The First Amendment protects religious freedom, speech, the press, the right to peaceably assemble, and the right to petition the government for a redress of grievances. The Fourth Amendment protects the people from unreasonable searches and seizures and requires that warrants be issued only upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched and the individual or things to be seized. The Sixth Amendment establishes the right of an accused individual to a speedy and public trial by an impartial jury, to be informed of the nature and cause of the charges, to confront witnesses, to have compulsory process to obtain witnesses, and to have the assistance of legal counsel. The Fourteenth Amendment addresses citizenship rights and equal protection of the laws. Although the equal protection clause applies explicitly only to state governments, equal protection requirements apply to the federal government through the Fifth Amendment Due Process Clause.

Appendix D—Sample Face Recognition Policy

The following is a sample face recognition policy that contains all of the sample policy language shown after each question in the template section (Chapter II) of this document. However, while drafting a face recognition policy that includes this language, it is important that the policy author review each question and its associated guidance in the template section while customizing this language. To facilitate this task, the policy language contained in this appendix mirrors the same structure and policy categories as those in the template so that the author can follow each template question, item by item, to customize this language.

It is critical that the policy author not cut and paste the policy language from this appendix (or from the template) and use it as is, without making modifications. There are many areas that prompt the author to insert or customize language. These are shown **bolded and in brackets [ ]**. It is also important to note that this sample policy may not cover all concepts that are unique to your entity's specific face recognition program, and there may be provisions that are not applicable that should be deleted. When developing their policies, law enforcement entities and fusion centers are encouraged to enhance the language with references to applicable statutes, rules, standards, guidelines, and policies.

Finally, since this guidance promotes transparency with the public, each entity should ensure that its policy is written in a manner that is understandable by both entity personnel and members of the public. While some of the provisions in this guidance may reflect concepts and processes long understood and integrated into the daily work of law enforcement such that an entity may not feel they are necessary to be included in its policy, the provisions are included in the sample policy for the purposes of informing the general public and articulating the entity's policies and procedures for P/CRCL throughout the entity face recognition program.

A. Purpose Statement

1. Facial recognition technology involves the ability to examine and compare distinguishing characteristics of a human face through the use of biometric algorithms contained within a software application. This technology can be a valuable investigative tool to detect and prevent criminal activity, reduce an imminent threat to health or safety, and help in the identification of persons unable to identify themselves or deceased persons. The **[name of entity]** has **[implemented or, if applicable, established access and use of]** a face recognition **[program or, if applicable, system]** to support the investigative efforts of law enforcement and public safety agencies both within and outside **[insert state name]**.

2. It is the purpose of this policy to provide **[name of entity]** personnel with guidelines and principles for the collection, access, use, dissemination, retention, and purging of images and related information applicable to the implementation of a face recognition (FR) program. This policy will ensure that all FR uses are consistent with authorized purposes while not violating the privacy, civil rights, and civil liberties (P/CRCL) of individuals.
   Further, this policy will delineate the manner in which requests for face recognition are received, processed, catalogued, and responded to. The Fair Information Practice Principles (FIPPs) form the core of the privacy framework for this policy.

This policy assists **[name of entity]** and its personnel in:

- Increasing public safety and improving state, local, tribal, territorial, and national security.
- Minimizing the threat and risk of injury to specific individuals.
- Minimizing the threat and risk of physical injury or financial liability to law enforcement and others responsible for public protection, safety, or health.
- Minimizing the potential risks to individual privacy, civil rights, civil liberties, and other legally protected interests.
- Protecting the integrity of criminal investigatory, criminal intelligence, and justice system processes and information.
- Minimizing the threat and risk of damage to real or personal property.
- Fostering trust in the government by strengthening transparency, oversight, and accountability.
- Making the most effective use of public resources allocated to public safety entities.

3. All deployments of the face recognition system are for official use only/law enforcement sensitive (FOUO/LES). The provisions of this policy are provided to support the following authorized uses of face recognition information.

[List any of the following that may be applicable and add any other authorized uses that apply to the entity. Note: Uses must be specifically authorized for your entity and must be in accordance with laws, statutes, policies, and procedures governing the entity.

- **A reasonable suspicion that an identifiable individual has committed a criminal offense or is involved in or planning criminal (including terrorist) conduct or activity that presents a threat to any individual, the community, or the nation and that the information is relevant to the criminal conduct or activity.**
- **An active or ongoing criminal or homeland security investigation.**
- **To mitigate an imminent threat to health or safety through short-term situational awareness surveillance or other means.**
- **To assist in the identification of a person who lacks capacity or is otherwise unable to identify him- or herself (such as an incapacitated, deceased, or otherwise at-risk person).**
- **To investigate and/or corroborate tips and leads.**
- **For comparison to determine whether an individual may have obtained one or more official state driver's licenses or identification cards that contain inaccurate, conflicting, or false information.**
- **To assist in the identification of potential witnesses and/or victims of violent crime.**
- **To support law enforcement in critical incident responses and special events.]**

[For those entities using mobile face image capture devices, there may be narrowly tailored purposes for use. Insert the following language and list the purposes that are applicable, and any others that are relevant, to the entity:

Mobile face image searches may be performed only by an officer who has completed training and only during the course of an officer's lawful duties in furtherance of a valid law enforcement purpose and in accordance with the conditions set forth in section F.7 (Refer to F. Use of Face Recognition Information, item 7). Some suggested valid law enforcement purposes include:

- **For persons who are detained for offenses that:**
  - **Warrant arrest or citation or**
  - **Are subject to lawful identification requirements and are lacking positive identification in the field.**
- **For a person who an officer reasonably believes is concealing his or her true identity and has a reasonable suspicion the individual has committed a crime other than concealing his or her identity.**
- **For persons who lack capacity or are otherwise unable to identify him- or herself and who are a danger to themselves or others.**
- **For those who are deceased and not otherwise identified.]**

B. Policy Applicability and Legal Compliance

1. This policy was established to ensure that all images are lawfully obtained, including face recognition probe images obtained or received, accessed, used, disseminated, retained, and purged by the **[name of entity]. This policy also applies to:**
   - Images contained in a known identity face image repository and its related identifying information.
   - **The face image** searching process.
   - Any results from face recognition searches that may be accessed, searched, used, evaluated, retained, disseminated, and purged by the **[name of entity]**.
   - Lawfully obtained probe images of unknown suspects that have been added to unsolved image files (refer to section L.3), pursuant to authorized criminal investigations.

2. All **[name of entity]** personnel, participating agency personnel, and authorized individuals working in direct support of **[name of entity]** personnel (such as interns), personnel providing information technology services to the **[name of entity]**, private contractors, and other authorized users will comply with the **[name of entity]**'s face recognition policy and will be required to complete the training referenced in section N.2. In addition, authorized **[name of entity]** personnel tasked with processing face recognition requests and submissions, must also complete the specialized training referenced in section N.3. An outside agency, or investigators from an outside agency, may request face recognition searches to assist with investigations only if **[insert applicable requirement(s) from those recommended below or insert the entity's established requirements:**
   - **Prior to making requests, the outside agency has a formalized agreement (e.g., a memorandum of understanding or an interagency agreement) between the [name of entity] and the outside agency and the agreement acknowledges that requesting investigators have an understanding of the training concepts listed in section N. Training, item 4.**
   - **The outside agency first provides examples of its applicable policies (e.g., privacy) and acknowledges in writing that its requesting investigators have an understanding of the training concepts listed in section N. Training, item 4.**
   - **The outside agency completes the [name of entity]'s training identified in section N. Training, item 4.**
   - **The outside agency is a law enforcement agency that is making the request based on a valid law enforcement purpose that falls within the authorized uses listed in section A. Purpose Statement, item 3. and the requestor provides a case number and contact information (requestor's name, requestor's agency, address, and phone number) and acknowledges an agreement with the following statement:**

     The result of a face recognition search is provided by the [name of entity] only as an investigative lead and IS NOT TO BE CONSIDERED A POSITIVE IDENTIFICATION OF ANY SUBJECT. Any possible connection or involvement of any subject to the investigation must be determined through further investigation and investigative resources.]

3. The **[name of entity]** will provide a printed or electronic copy of this face recognition policy to all:
   - **[name of entity]** and non-**[name of entity]** personnel who provide services
   - Participating agencies
   - Individual authorized users

   The **[name of entity]** will require both a written acknowledgement of receipt of this policy and a written agreement to comply with this policy and its applicable provisions.

4. All **[name of entity]** personnel, participating agency personnel, and authorized individuals working in direct support of **[name of entity]** personnel (such as interns or volunteers), personnel providing information technology services to the **[name of entity]**, private contractors, agencies from which **[name of entity]** information originates, and other authorized users will comply with applicable laws and policies concerning P/CRCL, including, but not limited to **[include a specific reference to any relevant state statutes or other binding state or local policy specific to face recognition systems, then provide**

a list of other applicable state and federal P/CRCL laws and/or include a reference to the section or appendix containing a list of applicable laws].

C. Governance and Oversight

1. Primary responsibility for the operation of the **[name of entity]**'s justice information systems, face recognition program and system, operations, and the coordination of personnel; the receiving, seeking, retention, evaluation, data quality, use, purging, sharing, disclosure, or dissemination of information; and the enforcement of this policy is assigned to the **[position/title]** of the **[name of entity]**.

2. The **[name of entity]**'s **[insert title]** will designate **[a face recognition administrator or face recognition unit or department who/that]** will be responsible for the following **[include any of the following responsibilities that apply to the face recognition administrator or other responsibilities:**
   - **Overseeing and administering the face recognition program to ensure compliance with applicable laws, regulations, standards, and policy.**
   - **Acting as the authorizing official for individual access to face recognition information.**
   - **Ensuring that user accounts and authorities granted to personnel are maintained in a current and secure "need-to-know" status.**
   - **Reviewing face recognition search requests, reviewing the results of face recognition searches, and returning the most likely candidates—or candidate images—if any, to the requesting agency.**
   - **Ensuring that protocols are followed to ensure that face recognition information (including probe images) is automatically purged in accordance with the entity's retention policy (refer to section L.1. Information Retention and Purging), unless determined to be of evidentiary value.**
   - **Ensuring that random evaluations of user compliance with system requirements and the entity's face recognition policy and applicable law are conducted and documented (refer to section M.2. Accountability).**
   - **Confirming, through random audits, that face recognition information is purged in accordance with this policy and to ensure compliance with applicable laws, regulations, standards, and policy.**
   - **Ensuring and documenting that personnel (including investigators from external agencies who may make face recognition search requests) meet all prerequisites stated in this policy prior to being authorized to use the face recognition system.]**

3. **[Select the option that is applicable to the entity.]**

   Option 1: The entity operates its own face recognition program.

   The **[name of entity]** face recognition program was established on **[date]** in conjunction with **[other agency partners, if applicable]**. Personnel from the following agencies are authorized to request face recognition searches:
   - **[Insert list of agencies authorized to request face recognition searches]**.

   Option 2: The entity has authorized access to a face recognition system.

   The **[name of entity]** has authorized access to and can perform face recognition searches utilizing the **[insert name of entity that owns the face recognition program]** face recognition system.

4. The **[name of entity]** contracts with **[insert name of commercial entity or vendor]** to provide **[insert applicable vendor role, such as "software and system development services for the entity's face recognition system"]**. The **[name of entity]** retains ownership of the face recognition system and the images and information it contains.

5. The **[name of entity]** is guided by a **[insert guiding authority, for example, a "designated face recognition oversight committee"]** that ensures that P/CRCL are not violated by this face recognition policy and by the **[name of entity]**'s face recognition information collection, receipt, access, use, dissemination, retention, and purging processes and procedures. The **[insert guiding authority, for example, a "designated face recognition oversight committee"]** engages with the community regarding **[name of entity]'s** face recognition policy prior to publishing.

   It is suggested that the committee will annually review and update the face recognition policy in response to changes in law and program implementation experience, including the results of audits and inspections, and may ***solicit input from the entity's stakeholders*** **[insert, if applicable "and may provide notice to and solicit comment from the public"]** on the development of the face recognition policy or proposed updates to the face recognition policy.

6. The **[insert title of individual or name of entity]** will:
   - Receive reports regarding alleged errors and violations of the provisions of this face recognition policy or applicable state law.
   - Receive and coordinate complaint resolution under the [name of entity]'s face recognition redress policy.
   - Ensure that the provisions of this policy and P/CRCL protections are implemented through efforts such as training, business process changes, and system designs that incorporate privacy-enhancing technologies.

   The **[insert title of individual but not the name or name of entity]** may be contacted at the following address: **[insert phone number, mailing address, or e-mail address]**, which is also posted on **[insert website where this information is listed for purposes of public redress]**.

7. The **[insert title of individual or name of entity]** will ensure that enforcement procedures and sanctions outlined in **[insert section number of policy (see Section M.3. Enforcement)]** are adequate and enforced.

D. Definitions

1. For examples of primary terms and definitions used in this face recognition policy, refer to **[insert section or appendix citation]**.

E. Acquiring and Receiving Face Recognition Information

1. **[Select all options that are applicable to the entity.]**

   Option 1: The entity maintains or operates an entity-owned image repository.

   The **[name of entity]** face recognition system can access and perform face recognition searches utilizing the following entity-owned face image repositories:
   - **[Insert a list of entity-owned and maintained repositories, including information types.]**

   Option 2: The entity has authorized access to and can perform face recognition searches utilizing image repositories not owned by the entity. Indicate the authority/source of the repository (e.g., driver's license photographs).

   The **[name of entity]** is authorized to access and perform face recognition searches utilizing the following external repositories:
   [List the image type and authority/source for each repository accessed. These may include:
   - **Mug-shot images [check state authority and insert source]**

- **Driver's license photographs [check state authority and insert source]**
- **State identification card photographs [check state authority and insert source]**
- **Sex Offender Registry [check state authority and insert source]**
- **[Specify any other image repositories that are accessed and cite state authority.]]**

Option 3: In addition to above, the entity is authorized to request that face recognition searches be performed by an external entity that operates a face recognition program.

In addition to above, the **[name of entity]** is authorized to submit requests for face recognition searches to be performed by the following external entities that own and maintain face image repositories:

[List the image type and authority/source for each repository accessed. These may include:

- **Mug-shot images [check relevant state authority and insert source]**
- **Driver's license photographs [check relevant state authority and insert source]**
- **State identification card photographs [check relevant state authority and insert source]**
- **Sex Offender Registry [check relevant state authority and insert source]**
- **[Specify any other image repositories that are accessed and cite state authority.]]**

2. For the purpose of performing face recognition searches, the **[name of entity]** and authorized **[name of entity]** personnel will obtain probe images or accept probe images from authorized requesting or participating agencies only for the authorized uses identified in section A.2.

3. The **[name of entity]** will receive probe images only from **[list other law enforcement agency or agencies]** in accordance with **[insert mechanisms, e.g., MOU, law, intergovernmental or interagency agreement]** established between the **[name of entity]** and the law enforcement agency(ies). If a non-law enforcement entity wants to submit a probe image for the purpose of a face recognition search, the entity will be required to file a criminal complaint with the appropriate law enforcement entity prior to the search.

4. The **[name of entity]** and, if applicable, any authorized requesting or participating agencies will not violate First, Fourth, and Fourteenth Amendments and will not perform or request face recognition searches about individuals or organizations based solely on their religious, political, or social views or activities; their participation in a particular noncriminal organization or lawful event; or their races, ethnicities, citizenship, places of origin, ages, disabilities, genders, gender identities, sexual orientations, or other classification protected by law.

However, the **[name of entity]** accords special consideration to the collection of face images relating to First Amendment-protected events, activities, and affiliations. Because of the sanctity of the First Amendment, law enforcement's role at First Amendment-protected events is usually limited to crowd control and public safety.[1] If, however, during the planning assessment and approval process for the particular event, before proceeding with the collection, the **[name of entity]** anticipates a need for the collection of face images, the **[name of entity]** will articulate whether collection of face images by law enforcement officers at the event is permissible; the legal or justified basis for such collection (including specifics regarding the criminal behavior that is suspected); and how face images may be collected, used, or retained, in accordance with this policy, as appropriate. If face images will be collected, the plan will specify the type of information collection that is permissible, identify who will collect face images (uniform or plainclothes officers), and define the permissible acts of collection.

[1] For further information about these processes, see *Recommendations for First Amendment-Protected Events for State and Local Law Enforcement Agencies* at 4, Global Justice Information Sharing Initiative, https://it.ojp.gov/GIST/35/Recommendations-for-First-Amendment-Protected-Events-for-State-and-Local-Law-Enforcement-Agencies.

[Note: Some law enforcement purposes may be stated generally in the Operations Plan or communicated to officers, but objectives that may risk interference with the exercise of First Amendment rights should be stated narrowly and be expressly tied to a specific law enforcement function (e.g., public safety, investigative).]

The use of mobile face image capture devices relating to First Amendment-protected events, activities, and affiliations will be specially authorized by **[title of entity supervisor/director/administrator]** of the **[name of entity]** in advance of the event.

The **[name of entity]** will reassess the need for and use of face recognition during the First Amendment-protected event. The **[name of entity]** will utilize face images from a First Amendment-protected event should the public safety mission change or in support of an active or ongoing criminal or homeland security investigation that occurs during or resulted from a First Amendment-protected event.

5. The **[name of entity]** will contract only with commercial face recognition companies or subcontractors that provide assurances that their methods for collecting, receiving, accessing, disseminating, retaining, and purging face recognition information comply with applicable local, state, tribal, territorial, and federal laws, statutes, regulations, and policies and that these methods are not based on unfair or deceptive information collection practices.

F. Use of Face Recognition Information

1. Access to or disclosure of face recognition search results will be provided only ***to individuals within the entity or in other governmental agencies*** who are authorized to have access or have completed applicable training outlined in section N. Training, and only for valid law enforcement purposes (e.g., enforcement, reactive investigations), and to IT personnel charged with the responsibility for system administration and maintenance. Authorized uses are described in A.3 of this policy. [**Insert, if applicable, any additional restrictions or allowances regarding the use of images in briefings or trainings, and whether there are any distinctions for hard-copy versus digital images.]**

2. The **[name of entity]** will prohibit access to and use of the face recognition system, including dissemination of face recognition search results, for the following purposes:
   - Non-law enforcement (including but not limited to personal purposes).
   - Any purpose that violates the U.S. Constitution or laws of the United States, including the protections of the First, Fourth, and Fourteenth Amendments.
   - Prohibiting or deterring lawful individual exercise of other rights, such as freedom of association, implied by and secured by the U.S. Constitution or any other constitutionally protected right or attribute.
   - Harassing and/or intimidating any individual or group.
   - Any other access, use, disclosure, or retention that would violate applicable law, regulation, or policy.

3. The **[name of entity] [does not/does]** connect the face recognition system to any interface that performs live video surveillance, including surveillance cameras, drone footage, and body-worn cameras. The face recognition system **[will not/will]** be configured to conduct face recognition analysis on live or recorded video.

4. The **[name of entity]** will employ credentialed, role-based access criteria, as appropriate, to control:
   - Categories of face recognition information to which a particular group or class of users may have access, based on the group or class.
   - The assignment of roles (e.g., administrator, manager, operator, and user).
   - The categories of face recognition information that a class of users are permitted to access, including information being utilized in specific investigations.
   - Any administrative or functional access required to maintain, control, administer, audit, or otherwise manage the information or equipment.

5. The following describes the **[name of entity]**'s manual and automated face recognition search procedure, which is conducted in accordance with a valid law enforcement purpose and this policy.
   - Authorized **[name of entity]** personnel **[and/or authorized requesting agency personnel]** will submit a probe image of a subject of interest.
   - Trained **[name of entity]** authorized examiners will initially run probe images without filters, using a filtered search as a secondary search, if needed. In some cases, enhancements may be considered after running an image as is against the image repository.
   - In the automated search, most likely candidates are returned to the requestor ranked in order based on the similarity or confidence level.
   - The resulting candidates, if any, are then manually compared with the probe images and examined by an authorized, trained examiner. Examiners shall conduct the comparison of images, biometric identifiers, and biometric information in accordance with their training.
     - If no likely candidates are found, the requesting entity will be informed of the negative results. In the case of a negative result, the images examined by the examiner will not be provided to the requesting entity.
   - Examiners will submit the search and subsequent examination results for a peer review of the probe and candidate images for verification by other authorized, trained examiners.
   - All results of most likely candidate images from the face recognition search must be approved by a supervisor prior to dissemination.
   - All entities receiving the results of a face recognition search must be cautioned that the resulting candidate images do not provide positive identification of any subject, are considered advisory in nature as an investigative lead only, and do not establish probable cause, without further investigation, to obtain an arrest warrant without further investigation.
   - The following statement will accompany the released most likely candidate image(s) and any related records:

     The **[name of entity]** is providing this information as a result of a search, utilizing face recognition software, of records maintained by the **[name of records entity]**. This information is provided only as an investigative lead and **IS NOT TO BE CONSIDERED A POSITIVE IDENTIFICATION OF ANY SUBJECT**. Any possible connection or involvement of any subject to the investigation must be determined through further investigation and investigative resources.

6. The **[name of entity]** has established the following process for mobile face recognition searches:
   - Only **[name of entity]** authorized and trained officers may utilize the mobile face recognition application and only on department-authorized devices. **[If personal devices are permitted, insert entity policy regarding use of mobile face recognition on personal devices.]**
   - Prior to utilizing a face recognition search, an officer should first attempt to ascertain an individual's identity by means other than a face recognition search, such as requesting identification, using a fingerprint scanner, etc.
   - Mobile searches may be performed during the course of an officer's lawful duties and only for the entity-established authorized uses listed in section A. Purpose Statement, item 3.
   - In addition, officers may only capture an individual's image when one of the conditions listed in section F.7 exist.
   - **[Use the following language, if the process is applicable to the entity. "The face recognition system does not work over standard cellular internet. Officers must log in and be authenticated into the [name of entity]'s law enforcement network in order to access the face recognition system."]**
   - The log-in screen will prompt the user to acknowledge and agree to the following statement before granting access to the system:
     - Face recognition is not a form of positive identification of a subject. Images returned as a result of a face recognition search may be considered investigative lead information only and are not probable cause to arrest, without further investigation.
     - Face recognition searches shall not be performed by the user on behalf of others who have not been trained and authorized to perform the searches.

    - All face recognition searches are subject to audit and require case numbers and file class/crime types.
    - Misuse may result in administrative and/or criminal penalties.
  - Prior to executing the search, the officer must enter the reason for the search within the application. **[List the reasons that are prompted by the entity's face recognition application. Reasons may include the following:**
    - **Consent**
    - **Reasonable suspicion of a crime**
    - **Probable cause**
    - **Physical/mental incapacity**
    - **Test/training**
    - **Other—[enter written reason]**
  - The captured image (probe image) will be submitted to the face recognition system, which will compare the probe image with those contained in the **[indicate the name(s) of repository/ies searched]**.
  - A list of most likely candidate images is returned ranked by computer-evaluated similarity.
  - The officer then completes a visual or manual morphological comparison of the candidate images with the subject's probe image to make a visual judgment, as well as uses standard investigative techniques, to determine whether the subject is the same as a candidate image.

7. Authorized and trained **[name of entity]** officers may only perform a mobile face recognition search during the course of lawful duties, in accordance with entity-established authorized uses (refer to section A. Purpose Statement, item 3), and when one of the following conditions exist:
   - Public Place: In accordance with applicable law, the individual's image is captured in a public place for the purpose of identification and the individual has no reasonable expectation of privacy. The **[name of entity]** will not authorize the collection of the individual's face image when the individual raises an objection that is recognized by law (e.g., religious objection).
   - Consent: The individual consents to have his or her image captured for the purpose of identification. The individual may withdraw consent at any time. If consent is withdrawn and neither of the other conditions applies, then use of a face recognition search is not authorized and the search must stop immediately.
   - Incapacitation, Defect, or Death: When an individual is unable to provide reliable identification because of physical incapacitation or defect, mental incapacitation or defect, or death, and an immediate identification is needed to assist the officer in the performance of his or her lawful duties.

8. At no time is the use of force permitted to capture a subject's image.

G. Sharing and Disseminating Face Recognition Information

1. The **[name of entity]** will establish requirements for external law enforcement agencies to request face recognition searches. These will be documented in an interagency agreement or MOU, which will include an assurance from the external agency that it complies with the laws and rules governing it, including applicable federal and state laws. The agreement will specify only those agency personnel who have been authorized by the **[name of entity]**, who have completed the required training identified in section N.2, and that requests are for official use only/law enforcement sensitive (FOUO/LES). Each request must be accompanied by a complaint number or case number.

2. The **[name of entity]**'s face recognition search information **will not** be:
   - Sold, published, exchanged, or disclosed to commercial or private entities or individuals except as required by applicable law and to the extent authorized by the **[name of entity]**'s agreement with the commercial vendor.
   - Disclosed or published without prior notice to the originating entity that such information is subject to disclosure or publication. However, the **[name of entity]** and the originating agency may agree in writing in advance that the **[name of entity]** will disclose face recognition search information as part

of its normal operations, including disclosure to an external auditor of the face recognition search information.
- Disclosed on a discretionary basis unless the originating agency has provided prior written approval or unless such disclosure is otherwise authorized by the MOU or agreement between the **[name of entity]** and the originating agency.
- Disclosed to unauthorized individuals or for unauthorized purposes.
- **[For commercial face recognition vendors, the entity should closely review its vendor agreement.]**

3. The **[name of entity]** will not confirm the existence or nonexistence of face recognition information to any individual or agency that would not be authorized to receive the information unless otherwise required by law.

H. Data Quality Assurance

1. Original probe images will not be altered, changed, or modified in order to protect the integrity of the image. Any enhancements made to a probe image will be made on a copy, saved as a separate image, and documented to indicate what enhancements were made, including the date and time of change.

2. **[Name of entity]** examiners will analyze, review, and evaluate the quality and suitability of probe images, to include factors such as the angle of the face image, level of detail, illumination, size of the face image, and other factors affecting a probe image prior to performing a face recognition search.

3. The **[name of entity]** considers the results, if any, of a face recognition search to be advisory in nature as an investigative lead only. Face recognition search results are **not** considered positive identification of a subject and do not, on their own, establish probable cause, without further investigation. Any possible connection or involvement of the subject(s) to the investigation must be determined through further investigative methods.

   [Add the following statement if the entity utilized mobile face recognition searches.

   All potential matches are considered advisory in nature and any subsequent verification of the individual's identity, such as through a fingerprint check, or follow-on action should be based on an agency's standard operating procedures.]

4. The **[name of entity]** will make every reasonable effort to perform routine maintenance, upgrades and enhancements, testing, and refreshes of the face recognition system to ensure proper performance, including the following:
   - Designated, trained personnel shall assess the face recognition system on a regular basis to ensure performance and accuracy.
   - Malfunctions or deficiencies of the system will be reported to the **[insert position/title]** within **[insert time period, e.g., number of days]** of discovering the malfunctions or deficiencies.

5. The integrity of information depends on quality control and correction of recognized errors which is key to mitigating the potential risk of misidentification or inclusion of individuals in a possible identification. The **[name of entity]** will investigate, in a timely manner, alleged errors and malfunctions or deficiencies of face recognition information or, if applicable, will request that the originating agency or vendor investigate the alleged errors and malfunctions or deficiencies. The **[name of entity]** will correct the information or advise the process for obtaining correction of the information.

I. Disclosure Requests

1. Face recognition information will be disclosed to the public in accordance with **[cite applicable state retention laws, public records laws, and policy]**. A record will be kept of all requests and of what

information is disclosed to an individual. **[If the state law prohibits disclosure, revise provision to reflect this.]**

J. Redress

J.1 Complaints

1. If an individual has a complaint with regard to face recognition information that is exempt from disclosure, is held by the **[name of entity]**, and allegedly has resulted in demonstrable harm to the complainant, the **[name of entity]** will inform the individual of the procedure for submitting (if needed) and resolving such complaints. Complaints will be received by the entity's **[Privacy Officer, Face Recognition Administrator, Internal Affairs Representative, or other position title]** at the following address: **[insert mailing address, e-mail address, and/or link to page if complaints can be submitted electronically]**. The **[Privacy Officer, Face Recognition Administrator, Internal Affairs Representative, or other position title]** will acknowledge the complaint and state that it will be reviewed but will not confirm the existence or nonexistence of the information to the complainant unless otherwise required by law.

   If the face recognition information did not originate with the entity, the **[Privacy Officer, Face Recognition Administrator, Internal Affairs Representative, or other position title]** will notify the originating agency within 30 days in writing or electronically and, upon request, assist such agency to correct any identified data/record deficiencies in the information or verify that the record is accurate.

   All face recognition information held by the entity that is the subject of a complaint will be reviewed within 30 days and confirmed or corrected/purged if determined to be inaccurate or incomplete, to include incorrectly merged or out-of-date information. If there is no resolution within 30 days, the entity will not share the information until such time as the complaint has been resolved. A record will be kept by the entity of all complaints and the resulting action taken in response to them.

J.2 Requests for Corrections

1. If, in accordance with state law, an individual requests correction of face recognition information *originating with the* **[name of entity]** that has been disclosed, the **[name of entity]**'s **[insert title of designee]** will inform the individual of the procedure for requesting a correction. The **[name of entity]** will investigate, in a timely manner, alleged errors and malfunctions or deficiencies of face recognition information or, if applicable, will request that the originating agency or vendor investigate the alleged errors and malfunctions or deficiencies. The **[name of entity]** will correct the information or advise the process for obtaining correction of the information. A record will be kept of all requests and the **[name of entity]**'s response.

J.3 Appeals

1. The individual who has requested disclosure or to whom face recognition information has been disclosed will be informed of the reason(s) why the **[name of entity]** or originating agency denied the request for disclosure or correction. The individual will also be informed of the procedure for appeal when the **[name of entity]** or originating agency has cited an exemption for the type of information requested or has declined to correct challenged face recognition information to the satisfaction of the individual to whom the information relates.

K. Security and Maintenance

1. The entity will comply with generally accepted industry or other applicable standards for security, in accordance with **[insert the name of the entity security policy or reference applicable standard(s)]** to protect data at rest, in motion, or in use. Security safeguards will cover any type of medium (printed or electronic) or technology (e.g., physical servers, virtual machines, and mobile devices) used in a work-related **[name of entity]** activity.

The **[name of entity and, if applicable, the name of entity's face recognition vendor]** will operate in a secure facility protected with multiple layers of physical security from external intrusion and will utilize secure internal and external security and privacy safeguards against network intrusions, such as strong multifactor authentication; encrypted communications; firewalls; and other reasonable physical technological, administrative, procedural, and personnel security measures to minimize the risks of unauthorized access to the system. Access to **[name of entity]** face recognition information from outside the facility will be allowed only over secure networks.

All results produced by the [name of entity] as a result of a face recognition search are disseminated by secured electronic means (such as an official government e-mail address). Non-electronic disseminations will be conducted personally or by phone with the requestor or designee.

2. All individuals with access to **[name of entity]**'s information or information systems will report a suspected or confirmed breach to the **[Privacy Officer, Face Recognition Administrator, or other position title]** as soon as possible and without unreasonable delay, consistent with applicable laws, regulations, policies, and procedures. This includes a breach in any medium or form, including paper, oral, and electronic.

Best Practice Language: [To the extent allowed by existing data breach notification law] Following assessment of the suspected or confirmed breach and as soon as practicable, the **[name of entity]** will notify the originating agency from which the entity received face recognition information of the nature and scope of a suspected or confirmed breach of such information.

[In addition to the above, the entity should identify any existing laws or policies governing its breach response procedures and, in accordance with these laws and policies, provide specific guidance on breach response procedures, including notification to individuals affected by the breach. Determine whether your state has a data breach notification law and select the appropriate provision.]

Option 1: State, Local, Tribal, or Territorial Data Breach Notification Law

The **[name of entity]** adheres to **[insert citation to applicable data breach notification law.]**. The **[name of entity]** will determine whether a data breach requires notification to an affected individual, in accordance with applicable laws, regulations, policies, and procedures.

Option 2: Office Management and Budget (OMB) Memorandum M-17-12, Preparing for and Responding to a Breach of Personally Identifiable Information (January 13, 2017), https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2017/m-17-12_0.pdf. For additional information on the development of incident response plans, entities may refer to DOJ's *Best Practices for Victim Response and Reporting of Cyber Incidents*, https://www.justice.gov/sites/default/files/opa/speeches/attachments/2015/04/29/criminal_division_guidance_on_best_practices_for_victim_response_and_reporting_cyber_incidents2.pdf.

[Where no applicable state, local, tribal, or territorial law exists, or where entities choose to supplement existing law or policy, M-17-12 may be used as a guide. Entities do not need to adopt OMB M-17-12 in full. Rather, entities should review OMB M-17-12 to determine which provisions are applicable and may adapt those provisions to the specific needs of the entity.]

The **[name of entity]** will adhere to breach procedures established by Office Management and Budget (OMB) Memorandum M-17-12 (January 13, 2017). The provisions adopted by the **[name of entity]** are cited below. In accordance with OMB M-17-12 **[insert citations to the sections and paragraphs of OMB M-17-12 that will be adopted]** and relevant laws,

regulations, policies, and procedures, the **[name of entity]** will determine if, when, and how to provide notification to potentially affected individuals and other relevant entities.

Option 3: No State Data Breach Notification Law and Entity Does Not Follow OMB M-17-12

a. Entity Follows an Existing Data Breach Notification Policy

The **[name of entity]** will adhere to the **[name of entity]**'s policy governing data breach notification. In accordance with **[insert citation(s) to the existing policy and procedures]**, the **[name of entity]** will **[insert excerpted language from the policy and procedures, as appropriate here]**. The **[name of entity]** will determine whether a data breach requires notification to an affected individual, in accordance with applicable laws, regulations, policies, and procedures.

b. Entity Does Not Have an Existing Data Breach Notification Policy

[Review and adapt the following template language to reflect the entity's data breach notification policy and procedures.]

When the **[Privacy Officer, Face Recognition Administrator, or other position title]** is notified of a suspected or confirmed breach, the **[Privacy Officer, Face Recognition Administrator, or other position title]** will determine whether the entity's response can be conducted at the staff level or whether a breach response team, consisting of the **[Privacy Officer, Face Recognition Administrator, or other position title, and others (e.g., individual with oversight responsibility for entity operation, the entity security officer, legal counsel, privacy oversight committee, and/or other designee(s))]** must be convened to respond to the breach. The **[Privacy Officer, Face Recognition Administrator, or other position title]**, in coordination with the breach response team, when applicable, will assess the risk of harm to individuals potentially affected by a breach (e.g., the nature and sensitivity of the personally identifiable information [PII] potentially compromised by the breach, the likelihood of access and use of PII, and the type of breach involved), evaluate how the entity may best mitigate the identified risks, and provide recommendations to the **[title of individual with oversight responsibility for entity operation]** on suggested countermeasures, guidance, or other actions.

The **[title of individual with oversight responsibility for entity operation]** will determine whether a data breach requires notification to an affected individual, in accordance with applicable laws, regulations, policies, and procedures. If required, the **[name of entity]** will notify an individual whose PII was or is reasonably believed to have been breached and access to which threatens physical, reputational, or financial harm to that person. If notice to the individual is required, it will be made promptly and without unreasonable delay following discovery of the breach. Notice will be provided consistent with the legitimate needs of law enforcement to investigate the breach or any measures necessary to determine the scope of the breach and, if necessary, to reasonably restore the integrity of any information system affected by the breach.

The **[Privacy Officer, Face Recognition Administrator, or other position title]** is responsible for developing and updating the entity's data breach response plan on an annual basis and in accordance with any changes in law, guidance, standards, agency policy, procedures, staffing, and/or technology; for maintaining documentation about each data breach reported to the entity and the entity's response; and for keeping entity administrators informed of the status of an ongoing response. The **[title of individual with oversight responsibility for entity operation]** will determine when the response to a breach is concluded, based on input from the **[Privacy Officer, Face Recognition Administrator, or other position title]**.

3. All face recognition equipment and face recognition software and components will be properly maintained in accordance with the manufacturer's recommendations, including routine updates as appropriate.

4. The **[name of entity or, if applicable, the name of the entity's face recognition vendor]** will store face recognition information in a manner that ensures that it cannot be modified, accessed, or purged except by personnel authorized to take such actions.

5. Authorized access to the **[name of entity]'s** face recognition system will be granted only to personnel whose positions and job duties require such access and who have successfully completed a background check and the training referenced in section N. Training.

6. Usernames and passwords to the face recognition system are not transferrable, must not be shared by **[name of entity]** personnel, and must be kept confidential.

7. The system administrator will ensure that all manufacturer-generated default passwords are replaced with secure passwords before web-based interfaces of the system become operational. User passwords must meet the following standards **[insert rules, such as no English words and a combination of upper and lowercase letters, numbers, and at least two special characters]**. Authorized users are not permitted to use the same password over time and are required to change their password every **[insert period of time]**.

8. Queries made to the **[name of entity]**'s face recognition system will be logged into the system identifying the user initiating the query. All user access, including participating agency access, and queries are subject to review and audit.

9. The **[name of entity]** will maintain an audit trail of requested, accessed, searched, or disseminated **[name of entity]**-held face recognition information. An audit trail will be kept for a minimum of **[specify the retention period for your jurisdiction/entity for this type of request]** of requests, access, and searches of face recognition information for specific purposes and of what face recognition information is disseminated to each individual in response to the request.

   Audit logs will include:
   [Provide a list of the information maintained in the audit log, such as:
   - **The name, agency, and contact information of the law enforcement user**
   - **The date and time of access**
   - **Case number**
   - **Probe images (refer to section L.5)**
   - **The specific information accessed**
   - **The modification or deletion, if any, of the face recognition information**
   - **The authorized law enforcement or public safety justification for access (criminal investigation, criminal intelligence, imminent threat, or identification), including a relevant case number if available. Note: The justification should be consistent with section E.]**

L. Information Retention and Purging

1. [Select all options that are applicable to the entity.]

Option 1: The entity maintains or operates an entity-owned image repository

All images contained within the **[name of entity]**'s **[name of image repository, e.g., mug shot repository]** will be stored for a period not to exceed **[insert a time frame]**. After **[insert time period]**, the information will be automatically purged in accordance with purging protocols (i.e., permanently removed from the repository). Refer to section K. Security and Maintenance, item 9, regarding face recognition information stored in audit logs.

Option 2: The entity has authorized access to and can perform face recognition searches utilizing image repositories not owned by the entity

Images accessed by the **[name of entity]** for face recognition searches, in accordance with section E.1, are not maintained or owned by the **[name of entity]** and are subject to the retention policies of the respective agencies authorized to maintain those images.

Option 3: The entity is authorized to request that face recognition searches be performed by an external entity that operates a face recognition program.

The **[name of entity]** is authorized to submit face recognition search requests, in accordance with section E.1, to external agencies that own and maintain face image repositories. The images searched are subject to the retention policies of the respective agencies that maintain or own the face image repositories.

Once a face recognition image is downloaded by **[name of entity]** personnel and incorporated into a criminal intelligence record or an investigative case file, the face recognition information is then considered criminal intelligence or investigative information and the laws, regulations, and policies applicable to that type of information or criminal intelligence govern its use.

Any images that do not originate with the **[name of entity]** will remain in the custody and control of the originating agency and will not otherwise be transferred to any other entity without authorization from the originating agency.

If the face recognition image has become or there is reason to believe that it will become evidence, including Rosario material or evidence that tends to inculpate or exculpate a suspect, in a specific criminal or other law enforcement investigation or action, the following provisions apply:

a. In those circumstances in which an image is identified as being Rosario material or having evidentiary value, the face recognition **[insert administrator or other title]** or designee will review the facts of the specific case and determine whether the image should be retained beyond the established retention period. If it is determined that it is reasonable to believe the image is Rosario material or has evidentiary value, the face recognition **[insert administrator or other title]** will authorize the transfer of the applicable image from the image repository to **[insert appropriate response; for example, "the entity's investigative case file," "the entity's case management system," or "a form of digital storage media (CD, DVD, etc.) or other portable storage device"]** and will purge the image from the repository.
b. Agencies requiring images be retained by the **[name of entity]** beyond the established retention period may make a formal, written request to the **[name of entity]** to extend retention. Each request must specify the need for extended retention, the circumstances surrounding the request, the requesting agency's case number, and a specific point of contact within the requesting agency. The **[name of entity]** reserves the right to grant or deny agency requests based on the information provided.

The **[name of entity]** retains the right to remove images from the repository earlier than the retention period, based on the limitations of information storage requirements and subject to any applicable record retention laws and statutory disclosure mandates. Early removal, however, will not be used as a means for intentionally interfering with a lawful complaint or a public records request. The retention period may be modified at any time by the **[name of entity]**, subject to applicable legal requirements.

2. Probe images are not enrolled (stored) in the image repository. Retention of probe images will be the same as for the type of file (criminal case file, criminal intelligence file), whether paper or electronic, in which the information is stored.

3. A lawfully obtained probe image of an unknown suspect *may* be added to an unsolved image file pursuant to an authorized criminal investigation. Images in an unsolved image file are periodically compared with those in an image repository (of known persons). If a most likely candidate meets a minimum threshold of computer-evaluated similarity results, the contributor of the probe image is notified and requested to validate the continued need to store the image or determine whether the image can be purged. Images enrolled in an unsolved image file will be validated on a periodic basis, at least every **[insert time period]**, by the contributors to ensure that the criminal investigation remains active and that the image remains relevant to the investigation. If, in accordance with this policy, the contributor has not validated the need to retain the image in the unsolved file, the image will be purged.

4. The list of most likely candidate images is not enrolled (stored) in the image repository. For **[name of entity]** investigations, the case agent will maintain the list of most likely candidates from a face recognition search within the case file.

5. Probe images and face recognition search results are saved within the entity's system audit log, for audit purposes only. The audit log is available only to the **[insert position, such as a face recognition administrator]** and will be purged within **[insert time period]**. The audit log is not searchable and face recognition searches cannot be performed using the audit log.

M. Accountability and Enforcement

M.1 Transparency

1. The **[name of entity]** will be open with the public with regard to face recognition information collection, receipt, access, use, dissemination, retention, and purging practices. The **[name of entity]**'s face recognition policy will be made available in printed copy upon request and posted prominently on the **[name of entity]**'s website **[or web page]** at **[insert web address]**.

2. The **[name of entity]**'s **[Privacy Officer, Face Recognition Administrator, or other position title]** will be responsible for receiving and responding to inquiries and complaints about the entity's use of the face recognition system, as well as complaints regarding incorrect information or P/CRCL protections in the image repository maintained and face recognition system accessed by the **[name of entity]**. The **[Privacy Officer, Face Recognition Administrator, or other position title]** may be contacted at **[insert mailing address or e-mail address]**.

M.2 Accountability

1. The **[name of entity]** will adopt and follow procedures and practices by which it can ensure and evaluate the compliance of users with the face recognition system requirements and with the provisions of this policy and applicable law. This will include logging access to face recognition information, may include any type of medium or technology (e.g., physical servers, virtual machines, and mobile devices) used in a work-related activity, and will entail periodic random auditing of these systems so as not to establish a discernable pattern that may influence users' actions. These audits will be mandated at least **[insert quarterly, semiannually, annually, or other time period]**, and a record of the audits will be maintained by the **[Privacy Officer, Face Recognition Administrator,**

or title of designee] of the **[name of entity]** pursuant to the retention policy. Audits may be completed by an independent third party or a designated representative of the **[name of entity]**.

Appropriate elements of this audit process and key audit outcomes will be compiled into a report and may be provided to command staff and oversight entities or governance boards.[2]

[Entities may also release a summary of findings to the public, pursuant to law or as a matter of discretion. If so, entities should consider the optional language below.]

Optional: The **[name of entity]** will provide an overview of audit findings to the public to enhance transparency with respect to P/CRCL protections built into the **[name of entity]**'s operations.

Note: Statistical data may be incorporated into the publication, but the entity should be mindful of operational considerations. Actual audit logs, statistical data, or summary findings may contain PII. No PII should be included in the summary of audit findings released to the public.

2. The **[name of entity]**'s personnel or other authorized users shall report errors, malfunctions, or deficiencies of face recognition information and suspected or confirmed violations of the **[name of entity]**'s face recognition policy to the **[name of entity]**'s **[insert title of Face Recognition Administrator]**.

3. The **[Privacy Officer, Face Recognition Administrator, or other position title]** will review and update the provisions contained in this face recognition policy annually and will make appropriate changes in response to changes in applicable law, technology, and/or the purpose and use of the face recognition system; the audit review; and public expectations.

M.3 Enforcement

1. If **[name of entity]** personnel, a participating agency, or an authorized user is found to be in noncompliance with the provisions of this policy regarding the collection, receipt, access, use, dissemination, retention, and purging, the **[title of entity director]** of the **[name of entity]** will:
   - Suspend or discontinue access to information by the **[name of entity]** entity personnel, the participating agency, or the authorized user.
   - Apply appropriate disciplinary or administrative actions or sanctions.
   - Refer the matter to appropriate authorities for criminal prosecution, as necessary, to effectuate the purposes of the policy.

2. The **[name of entity]** reserves the right to establish the qualifications and number of personnel having access to the **[name of entity]**'s face recognition system and to suspend or withhold service and deny access to any participating agency or participating agency personnel violating this face recognition policy.

N. Training

1. Before access to the **[name of entity]**'s face recognition system is authorized, the **[name of entity]** will require the following individuals to participate in training regarding implementation of and adherence to this face recognition policy:
   - All authorized **[name of entity]** personnel, including examiners
   - All authorized participating agency personnel
   - All authorized personnel providing information technology services to the **[name of entity]**

[2] *Privacy, Civil Rights, and Civil Liberties Audit Guidance for the State, Local, Tribal, and Territorial Intelligence Component*, Global Justice Information Sharing Initiative, https://it.ojp.gov/GIST/181/Privacy--Civil-Rights--and-Civil-Liberties-Audit-Guidance-for-the-State--Local--Tribal--and-Territorial-Intelligence-Component.

2. The **[name of entity]**'s face recognition policy training program will cover both:
   a. Elements of the operation of the face recognition program, including:
      - Purpose and provisions of the face recognition policy.
      - Substance and intent of the provisions of this face recognition policy and any revisions thereto relating to collection, receipt, access, use, dissemination, retention, and purging of the **[name of entity]**'s face recognition information.
      - Policies and procedures that mitigate the risk of profiling.
      - How to implement the face recognition policy in the day-to-day work of the user, whether a paper or systems user.
      - Security awareness training.
      - How to identify, report, and respond to a suspected or confirmed breach.
      - Cultural awareness training.
   b. Elements related to the results generated by the face recognition system, including:
      - Originating and participating agency responsibilities and obligations under applicable federal, state, or local law and policy.
      - The P/CRCL protections on the use of the technology and the information collected or received, including constitutional protections, and applicable state, local, and federal laws.
      - Face recognition system functions, limitations, and interpretation of results.
      - Mechanisms for reporting violations of **[name of entity]** face recognition policy provisions.
      - The nature and possible penalties for face recognition policy violations, including possible transfer, dismissal, criminal liability, and immunity, if any.

3. In addition to the training described in M.2, the **[name of entity]** face recognition examiners are required to complete advanced specialized training to include:
   - Face recognition system functions, limitations, and interpretation of results.
   - Use of image enhancement **[if applicable, "and video editing software"].**
   - Appropriate procedures and how to assess image quality and suitability for face recognition searches.
   - Proper procedures and evaluation criteria for one-to-many and one-to-one face image comparisons.
   - Candidate image verification processes.

4. Investigators from outside agencies are permitted to request face recognition searches from the **[name of entity]**, only if prior to making requests the outside agency **[select applicable entity requirement(s) from the following list or insert the entity's established requirements:**
   - **There is a formalized agreement, (e.g., a memorandum of understanding or an interagency agreement), between the [name of entity] and the outside agency and the agreement acknowledges that requesting investigators have an understanding of the following concepts.**
   - **The outside agency first provides examples of its applicable policies (e.g., privacy) and acknowledges in writing that its requesting investigators have an understanding of the following concepts.**
   - **There is a law enforcement agency that is making the request based on a valid law enforcement purpose that falls within the authorized uses listed in section A. Purpose Statement, item 3. And the requestor provides a case number and contact information (requestor's name, requestor's agency, address, and phone number), and acknowledges an agreement with the following statement:**

     The result of a face recognition search is provided by the [name of entity] only as an investigative lead and IS NOT TO BE CONSIDERED A POSITIVEI IDENTIFICATION OF ANY SUBJECT. Any possible connection or involvement of any subject to the investigation must be determined through further investigation and investigative resources.

   - **The agency completes the [name of entity]'s training on the following concepts:**
     - **Originating and participating agency responsibilities and obligations under applicable federal, state, or local law and policy.**
     - **P/CRCL protections on the use of the technology and the information collected or received.**

- **Conditions and criteria under which the face recognition searches may be requested.**
- **Face recognition system functions, limitations, and interpretation of results.**
- **Use of face recognition search results as an investigative lead only.**
- **Mechanisms for reporting violations of [name of entity] face recognition policy provisions.**
- **The nature and possible penalties for face recognition policy violations, including dismissal, criminal liability, and immunity, if any.**
- **Operational policies.]**

5. In addition to the training described in N.2, the **[name of entity]** requires all personnel who are authorized to run a mobile search to be trained in the following areas prior to utilizing mobile face recognition search capabilities:

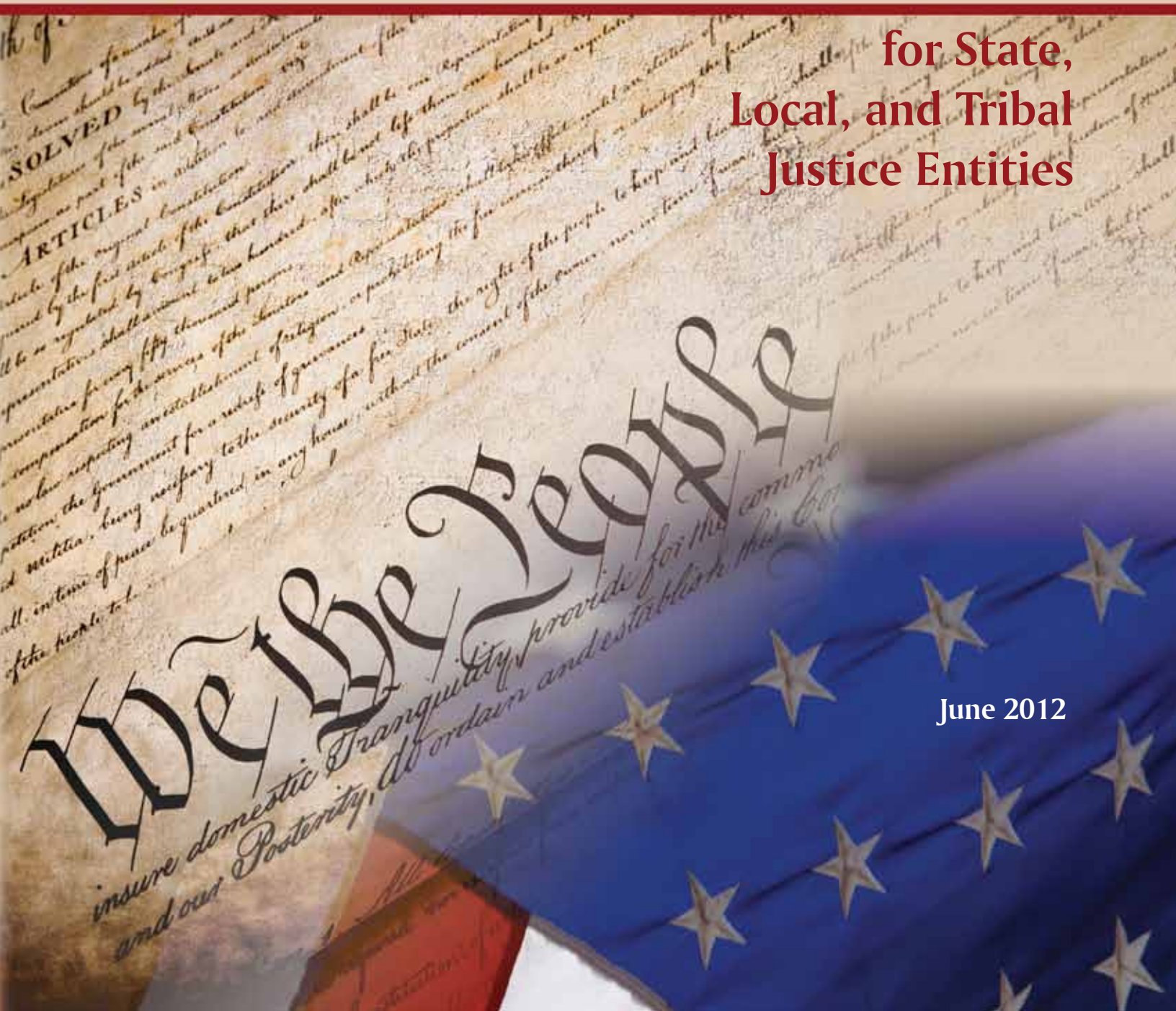
- The proper and lawful use of face images for face recognition purposes.
- How to capture high quality face images in the field for most accurate results.
- The rules and procedures for obtaining an individual's consent to having their image captured.
- The appropriate use and sharing of information obtained from a face recognition search.
- The deletion of field-acquired probe images.

Personnel who have not received this training shall not utilize mobile face recognition search capabilities.

Bureau of Justice Assistance
U.S. Department of Justice

Global Justice Information Sharing Initiative

Guide to Conducting Privacy Impact Assessments for State, Local, and Tribal Justice Entities



June 2012

Guide to Conducting Privacy Impact Assessments for State, Local, and Tribal Justice Entities

Where to Locate These Resources

The Global Privacy Resources featured within this guide and others are available online at www.it.ojp.gov/privacy. To request printed copies, send requests to GLOBAL@iir.com.

About the Global Advisory Committee

www.it.ojp.gov/global

The Global Advisory Committee (GAC) serves as a Federal Advisory Committee to the U.S. Attorney General. Through recommendations to the Bureau of Justice Assistance (BJA), the GAC supports standards-based electronic information exchanges that provide justice and public safety communities with timely, accurate, complete, and accessible information, appropriately shared in a secure and trusted environment. GAC recommendations support the mission of the U.S. Department of Justice, initiatives sponsored by BJA, and related activities sponsored by BJA's Global Justice Information Sharing Initiative (Global). BJA engages GAC-member organizations and the constituents they serve through collaborative efforts, such as Global working groups, to help address critical justice information sharing issues for the benefit of practitioners in the field.

About GPIQWG

www.it.ojp.gov/gpiqwg

The Global Privacy and Information Quality Working Group (GPIQWG) is one of four Global working groups. GPIQWG is a cross-functional, multidisciplinary working group of Global and is composed of privacy and local, state, tribal, and federal justice entity representatives covering critical topics such as intelligence, biometrics, information quality, privacy, civil rights, and civil liberties. GPIQWG assists government entities, institutions, and other justice agencies in ensuring that personally identifiable information is appropriately collected, maintained, used, and disseminated within evolving integrated justice information systems.

GPIQWG, on behalf of Global, developed this overview to support justice agencies in their efforts to balance the interests of law enforcement and public safety with the privacy rights and concerns of affected persons. For more information on GPIQWG, refer to: www.it.ojp.gov/gpiqwg.

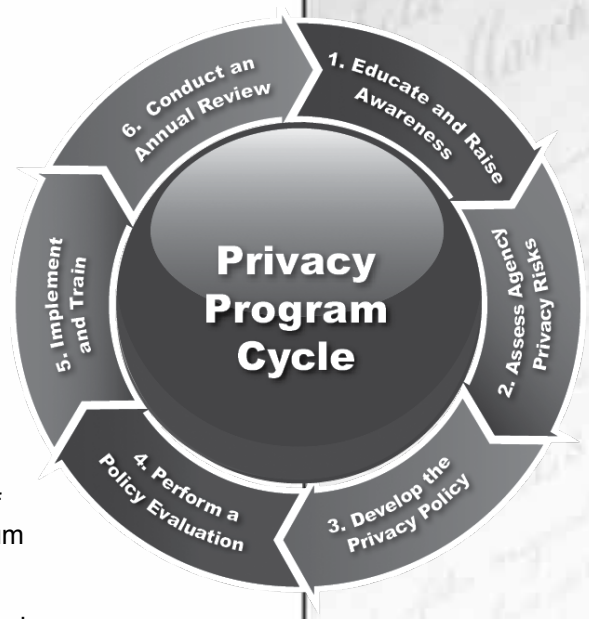
This project was supported by Grant No. 2011-D6-BX-K055 awarded by the Bureau of Justice Assistance, Office of Justice Programs, U.S. Department of Justice, in collaboration with the Global Justice Information Sharing Initiative. The opinions, findings, and conclusions or recommendations expressed in this publication are those of the author(s) and do not necessarily reflect the views of the U.S. Department of Justice.

Table of Contents

Introduction

This *Guide to Conducting Privacy Impact Assessments for State, Local, and Tribal Justice Entities* (or "PIA Guide") allows practitioners at state, local, and tribal (SLT) justice entities to examine the privacy implications of their information systems and information sharing collaborations so they can design and implement policies to address vulnerabilities identified through the assessment process.

The Global Justice Information Sharing Initiative (Global) develops resources to support justice entities in their efforts to develop and implement privacy, civil rights, and civil liberties policies and protections in their information sharing initiatives.



I. Privacy Program Cycle

Global has developed a flexible suite of products for every stage of an entity's privacy program cycle, each designed to meet a spectrum of privacy protection needs.

Stage 1—Educate and Raise Awareness on the importance of having privacy, civil rights, and civil liberties protections within the agency.

Stage 2—Assess Agency Privacy Risks by evaluating the process through which your agency collects, stores, protects, shares, and manages information.

Stage 3—Develop the Privacy Policy to articulate the policy position of an organization on how it handles information the agency seeks or receives and uses in the normal course of business.

Stage 4—Perform a Policy Evaluation to determine whether the privacy policy adequately addresses current standards and privacy protection recommendations.

Stage 5—Implement and Train personnel and authorized users on the established rules and procedures.

Stage 6—Conduct an Annual Review and make appropriate changes in response to applicable laws, technology, and public expectations.

This PIA Guide serves as the primary resource for **Stage 2—Assess Agency Privacy Risks.** Applying the privacy concepts discussed in Global *Privacy, Civil Rights, and Civil Liberties Policy Development Guide for State, Local, and Tribal Justice Entities* (Privacy Guide), the PIA Guide helps entities prepare for drafting a privacy policy by identifying privacy risks associated with the entity's information sharing system. Once the PIA is complete, entities are encouraged to refer to resources at Stage 3—Develop the Privacy Policy for tools to assist in the policy development process. For more information on all of the privacy resources available for each stage of an entity's Privacy Program Cycle, refer to DOJ's ***Global Privacy Resources*** booklet, available at www.it.ojp.gov/privacy.

Terms and Definitions

Familiarity with the following three terms will be helpful as you review this guide. Refer to Appendix B for terms and definitions.

Personally Identifiable Information (PII): Information from which an individual can be uniquely identified, such as name, address, date of birth, and social security number, and any information linked or linkable to the individual.

Privacy Impact Assessment (PIA): A series of questions that evaluate the processes through which personally identifiable information is collected, stored, protected, shared, and managed by an electronic information system or online collection application.

Privacy Policy: A legally binding notice of how an agency handles an information contributor's personal data. The privacy policy should contain details about collecting information and secondary uses of data, including how information is shared with third parties and who those third parties are.

II. Background

Information may be the wild card in the justice enterprise deck. Its expanded utility, made possible in large part by advances in information technology, strengthens public safety and supports the development and growth of SLT and regional justice information sharing initiatives.

However, inappropriate or reckless use of information can cause demonstrable harm by irreparably damaging reputations, threatening individual liberty, placing personal safety at risk, or denying individuals access to some of life's most basic necessities, such as employment, housing, and education.

Justice entity pursuit of information sharing capabilities must be accompanied equally by responsibility for the privacy, civil rights, and civil liberties protections of the information being used and exchanged. Information is maximized to its full potential only when it is used in the most responsible manner possible, with carefully designed privacy protections that recognize not only the tremendous benefits that information sharing can provide but also the damages that can occur when information is used and exchanged in a manner that conflicts with common expectations of privacy and confidentiality.

While the E-Government Act of 2002[1] resulted in significant federal-level privacy policy activity, particularly in PIA use for new or significantly modified federal information technology (IT) systems, there has been little activity on the state, local, or tribal fronts in privacy policy development or PIA use to examine IT system privacy vulnerabilities.

This risk assessment—more commonly known as a **Privacy Impact Assessment or PIA**—is a crucial first step in successful privacy policy development. A PIA allows leaders of an information sharing initiative to analyze privacy risks and exposures of data stored and exchanged by organizations participating in multijurisdictional information collaborations. Resulting policies specifically address these risks.

III. What Is Contained Within This Guide?

This guide provides the following:

- A PIA overview.
- A PIA template that leads practitioners through appropriate privacy risk assessment questions. The template is provided as Appendix A.
- A glossary of relevant terms and definitions in Appendix B.
- Two methods to institutionalize the PIA process for information systems development: model legislation and a draft governor's executive order. Model legislation is provided as Appendix C, and the draft executive order as Appendix D.
- OMB guidance for implementing the E-Government Act of 2002 in Appendix E.

1 Office of Management and Budget Memorandum (OMB M-03-022), *OMB Guidance for Implementing the Privacy Provision of the E-Government Act of 2002*, contained in Appendix E.

PIA Overview

I. What Is a PIA?

A Privacy Impact Assessment allows entities to adequately assess privacy risks in their information sharing initiatives. It lays the groundwork for comprehensive and effective privacy, civil rights, and civil liberties policies to protect information and its use while maximizing technological infrastructures and data sharing opportunities.

Taking a cue from Congress' E-Government Act, which requires PIAs for new or significantly modified federal IT systems, a PIA supports the notion that before diving into full privacy policy development, state, local, and tribal jurisdictions should first identify, analyze, and assess the risks associated with information systems when it comes to the privacy of the data and information they store and share. Once risks are identified and analyzed, policies can specifically address and mitigate them.

A PIA evaluates privacy implications when information systems are created or when existing systems are significantly modified. PIAs can also be conducted for existing IT systems that fall into neither of these two categories. Routine PIA use is a cost-effective demonstration of sound public policy.

II. The PIA Process

The following briefly highlights the PIA process.

1. The PIA process begins with the completion of a Privacy Threshold Analysis (PTA) to determine which systems actually need a PIA. This analysis will identify information that will be exchanged, with whom it will be exchanged, and whether there are any associated privacy, civil rights, or civil liberties implications.
2. Next, the PIA poses a series of questions that help stakeholders identify and understand any risks their systems may pose to the privacy, civil rights, and civil liberties of personally identifiable information.
3. Privacy policies emerge as the result of the identification and analysis that occur during the PIA process, generating discussion and decision making on how to address and mitigate, if necessary, the identified privacy vulnerabilities.

III. Why Is a PIA Important?

Protecting information privacy and associated legal rights is a foundational concept. Information systems used by law enforcement and other justice disciplines are perhaps more closely scrutinized than other government or privately operated information systems; therefore, they are held to higher standards.

Higher standards are expected for information that can deprive individuals of their personal freedom or that can put individuals such as victims and witnesses at risk. Additionally, criminal justice data is often collected without the consent of a data subject, who may be an alleged offender, a crime victim, or a witness. Greater diligence in data handling is crucial for safeguarding the interests of individuals who have little or no choice about becoming involved in the criminal justice system.

Essential to American democracy is the ability to hold government accountable for its actions through a variety of state and federal transparency laws that allow citizens to gain access to public meetings and official records.

Conducting a PIA illustrates an SLT entity's commitment to and thoughtful analysis of protection of the public's information. Maintaining public trust is at the core of the PIA concept; this is particularly true for criminal justice entities. The public must be assured that personal and confidential data will be collected and used lawfully. There are many practical and philosophical reasons to conduct a PIA. Addressing privacy concerns early in the design process can encourage policymaker support, as well as financial support, for a system. An effective PIA process may not gain public support but is likely to stimulate healthy debate and deflate potential opposition to important information sharing capabilities.

Failing to recognize privacy values can result in system shutdown, forced data destruction, costly modifications, implementation delays, and more restrictive legislative mandates, as well as personal and agency embarrassment.

Primarily, however, a PIA should be conducted to ensure that personal and confidential information entrusted to an agency is protected to the highest degree possible, sparing record subjects—whose interaction with the justice system is already almost assuredly causing tension—further trauma or even victimization by the improper use and exchange of their data.

State PIA Example—Alabama

The Alabama Criminal Justice Information Center (ACJIC) conducts privacy impact analyses of information shared through its Law Enforcement Tactical System (LETS) portal. LETS allows authorized criminal justice users to receive federated query results from multiple databases, including driver's license details, vehicle registrations, boat registrations, sex offender registry information, Department of Corrections information, court filings, dispositions, etc. Since 2010, it has been the official policy of the ACJIC Commission to post all PIAs related to information shared via LETS on ACJIC's public Web site at www.acjic.alabama.gov/about_pia.cfm.

Posting the PIAs online allows members of the public to learn how information contained within various governmental databases may be used for criminal justice purposes and explains the privacy and security safeguards that ACJIC has implemented to protect citizens' personally identifiable information (PII).

IV. When to Perform a PIA

As mentioned earlier, a PIA can be conducted to evaluate privacy implications when information systems are created, when existing systems are significantly modified, and also at any other time. In general, PIAs should be performed and updated as necessary where a system change creates new privacy, civil rights, and civil liberties risks. Appendix E provides a detailed list of these conditions, as recommended by the Office of Management and Budget.

You should first conduct two fundamental analyses to determine whether your system needs a PIA:

- First, analyze your system and information sharing initiative itself—basically by asking this simple question: "Which systems might need a PIA?" See A. for more information.
- Then, conduct a Privacy Threshold Analysis (PTA), to determine whether your system collects personally identifiable information (PII). See B. for more information.

A. Which Systems Need a PIA?

Examine your information system(s) and the information sharing initiative itself. The question is, Which systems need a PIA? The answers are easy: generally, any new data system—especially any new information sharing initiative—that collects PII should be subjected to a PIA as part of the planning process. In addition, any significant modification of an existing system should be the subject of a PIA if the modifications are associated with the collection, use, access, or dissemination of PII.

Therefore, determining whether your system(s) collect personally identifiable information—information from which an individual can be uniquely identified, such as name, address, date of birth, social security number, and any information linked or linkable to the individual—is the second fundamental analysis you need.

State PIA Example—Minnesota

A PIA conducted by Minnesota's Bureau of Criminal Apprehension on its eCharging Services Project raised the following questions:

- Does the data classification of incident report drafts change after a final incident report is submitted to the prosecutor?
- Does the action a prosecutor chooses to take on an incident change its data classification?
- Since eCharging will be deployed in phases, does it need different or temporary data classifications for its pilot project?

B. Privacy Threshold Analysis

If in doubt as to whether a PIA is appropriate, performing a **Privacy Threshold Analysis (PTA)** will help ascertain whether a PIA is needed for system upgrades or improvements. The first question is, Does the system store, use, or otherwise maintain personally identifiable information? If your answer is yes, consider the following:

Privacy Threshold Question 1: What information about individuals could be collected, generated, or retained?

Rationale. Creating a list of the types of PII a system will use requires that designers appropriately consider the types of PII data their systems will collect. Obvious types are name, address, or social security number. Less obvious types are information that can be linked or that is linkable to specific individuals. Note that information about individuals can even include their images captured by cameras monitoring specific locations or information about health status that may be detected by a system designed to capture radioactivity levels and thus determine whether an individual received chemotherapy. Privacy can be threatened when seemingly innocuous pieces of personal information—such as individual preferences that facilitate a Web site's use or proof of age on driver's licenses shown for participation in a separate age-restricted activity—are "bundled" in a single record. Privacy can also be endangered by the use of global positioning devices, cell phones, personal digital assistants, surveillance cameras, radio frequency identification tags, home wireless networks, and other technologies that could be monitored to provide information on where a person lives or works.

Privacy Threshold Question 2: Does your system operate under specific or general legal authority?

Rationale. Many agencies operate systems under their general statutory or other legal operating authority.[2] Some operate under specific legislation or regulation applicable to their information systems. You must determine whether either of these two conditions exists and ensure that your assessment and resulting privacy policy are in compliance with the provisions of any such laws or regulations. Be aware, however, that some statutes might not adequately address the privacy of the information collected. If no such specific regulations exist in your jurisdiction or the statute or regulation does not adequately address privacy, at minimum you should

2 Where applicable, you should consider what impact tribal privacy laws may have with regard to information collected, generated, maintained, or distributed by tribal government agencies. Tribal users may also want to consult the Indian Civil Rights Act of 1968, United States Code, Title 25, Chapter 15, Subchapter I, § 1301

State PIA Example—Ohio

Privacy Impact Statements and Assessments

In Ohio, commitment to the detection of privacy risks and assurance of privacy protections for the personally identifiable information (PII) state agencies handle is demonstrated by Ohio state law, as follows:

"To ensure privacy is considered, state agencies are required to create privacy impact statements in accordance with Section 125.18 [C][2] of the Ohio Revised Code (ORC)…a Privacy Impact Assessment (PIA) is [considered] the same as a privacy impact statement. Section 1347.15[B][8] of the Ohio Revised Code also requires state agencies to complete privacy impact assessment forms. [In addition,] Each state agency is required to have a Data Privacy Point of Contact (DPPOC) to assist the agency's program unit in completing a PIA.

"Furthermore, performing a PIA upon the collection of new types of information or at the beginning of the development or acquisition of a new information system that maintains PII will help a state agency to determine most, if not all, of the necessary privacy and security controls." *

This PIA process penetrates agencies statewide, such as the Ohio Department of Public Safety and many others that handle confidential personal information. Ohio even goes one step further by performing compliance checks administered by the Ohio state auditor.

* www.privacy.ohio.gov/Government.aspx, Ohio.gov, Privacy and Security Web site.

align your privacy policy with best practices as enumerated in the various existing state and federal laws, such as the Federal Privacy Act[3] and the Code of Federal Regulations.

Privacy Threshold Question 3: Has a PIA ever been conducted on your information system?

Rationale. PIAs are generally conducted at the beginning of an information system's design phase or when a system undergoes a significant upgrade. However, if your system collects, maintains, or generates PII, it would be wise to conduct a PIA even if your system does not fall into these two categories. A PIA will identify the privacy implications and characteristics of your IT system and will allow you to mitigate privacy vulnerabilities before a breach occurs. Your answers to these questions will reveal the privacy policy needs of your system and will help you to decide whether to continue on to a full PIA.

V. Steps to Developing the Privacy Policy: Where the PIA Fits In

Step 1 Systems and Privacy Threshold Analyses.

Analyze the information system and information use, maintenance, and sharing to determine which systems need a PIA. Then, conduct a PTA for each system. Take these additional steps after determining your system or information sharing initiative's privacy policy needs:

Step 2 Identify and analyze your shared information.

It is important to articulate the information exchanges that will occur in your system in order to understand how information will be shared across the system and with participating organizations. Knowing the agencies and organizations involved, what data they will share, when and under what circumstances it will be shared, and what the information will be used for is critical in understanding any privacy implications. It helps to follow a consistent, intuitive approach to capturing information-exchange requirements. For example, for each exchange, identify who is involved (what agencies/organizations), why the exchange is taking place (business process), when it takes place (business events and conditions), and what information is being exchanged. All of this analysis can be useful in understanding potential privacy risks, as well as in specifying privacy rules within a privacy policy. For more information on resources available to assist entities in analyzing information exchanges, refer to the Global Privacy Guide, Section 7. Understanding Information Exchanges.[4]

Step 3 Conduct the PIA. (Use the template contained in Appendix A.)

Step 4 Develop your privacy, civil rights, and civil liberties policies.

Use the Global Privacy Guide and SLT Policy Development Template, referenced earlier, to develop the content of your entity's privacy, civil rights, and civil liberties policy.[5]

3 Privacy Act of 1974, 5 U.S.C. § 552a, United States Code, Title 5, Part I, Chapter 5, Subchapter II, § 552a.
4 Global Privacy Guide, available at www.it.ojp.gov/privacy.
5 Ibid.

VI. Should You Publicize the Completed PIA?

A completed PIA can be a valuable public relations tool to proactively address privacy and other identified concerns as a system nears implementation. Prominent posting of a completed PIA on a Web site or at an agency's office allows the public and policymakers to evaluate its thoroughness and accuracy. The PIA also demonstrates an agency's role as a trusted data steward. An agency may also consider other methods, such as press releases, to increase public awareness of its completed PIA.

VII. Who Conducts the PIA?

Fundamental to information sharing system development are (1) agreement on guiding principles and (2) identification of strategic and tactical issues. Conducting a PIA during the strategic planning process ensures that privacy issues are addressed early and are accommodated in the system design and governance. Ideally, a PIA is completed by information system stakeholders (the governance group) as part of a strategic planning process and in collaboration with the agency's legal counsel, record managers, those responsible for data privacy, those responsible for freedom of information responses, and system security personnel.

The completed PIA is then submitted to the information system's governing/decision-making body. PIA results will show decision makers which policies are needed or any other work that might be necessary. In smaller organizations or information systems efforts, PIA responsibilities may belong to an individual rather than to a group; nevertheless, smaller agencies may still wish to include stakeholders and other individuals from outside their agencies to assist in PIA preparation. They can identify privacy issues and suggest ways to mitigate them. Interested and/or affected parties to supplement internal agency resources could include:

- Privacy advocates
- Private/public records managers
- Civil liberties organizations
- Elected officials
- Legislative research staff
- IT associations
- Other justice IT professionals
- Prosecutors
- Public defenders
- Judges
- Corrections, probation, and parole professionals

There may be other interested groups in addition to those listed above, such as public safety-minded local businesses, that could provide technical resources. A local hospital or medical provider may have a Health Insurance Portability and Accountability (HIPAA) expert whose knowledge in protecting health information could be useful in assessing your system's privacy implications. If no local civil liberties groups or public defenders are available, nonprofit organizations with outreach efforts around social justice issues, such as local churches and faith communities, could assist. In addition to gaining valuable expertise, allowing stakeholders to participate in the PIA preparation process demonstrates an agency's commitment to inclusiveness and openness. Ultimately, the PIA process should be as inclusive as possible to address the perspectives of members of the public who may be affected by the system. Including stakeholders in your review process gives you an opportunity to address their privacy concerns and may even eliminate some.

A Note About Resources

The authors of this guide acknowledge that, initially, the PIA process may seem too complex or time-intensive for rural agencies and smaller departments that may have limited resources to devote to this task. It is important to remember that in order to adequately analyze agency privacy risks, each question in the template contained in Appendix A will need to be addressed and answered. One way for smaller agencies to do this may be to pool resources for the purpose of completing the PIA. Bringing together individuals from a number of small agencies who each, according to their respective positions and varying responsibilities, utilize the information system being assessed will be helpful in completing the PIA process when none of the agencies have the resources to conduct a comprehensive PIA on their own. If appropriate, the entity may also consider reaching out to local professional associations (for law enforcement, for example, this may be sheriffs or police chiefs associations) or other organizations for assistance.

Ultimately, it is the responsibility of the governing body in a multiorganizational effort or of the agency executive in a smaller initiative to address the risks revealed by the PIA. These leaders will then determine whether the risks are acceptable, can be mitigated via policy development, or could result in a decision not to move forward with the project.

VIII. PIA Components

At minimum, a PIA should analyze and describe:

- Information to be collected (e.g., nature and source).
- Why information is being collected (e.g., to determine eligibility).
- Intended use of the information (e.g., to verify existing data).
- With whom the information will be shared (e.g., another agency for a specified programmatic purpose).
- What opportunities individuals have to decline to provide information (i.e., where providing information is voluntary) or to consent to particular uses of the information (other than required or authorized uses) and how individuals can grant consent. (Note: This is of particular importance, since collection of criminal justice data is often not voluntary or provided with consent.)
- How the information will be secured.

IX. PIA Outcome

A completed PIA should:

- Identify privacy, civil rights, and civil liberties vulnerabilities and risks for stakeholders, owners, entity heads, and others accountable for a system's operation.
- Include a summary of mitigating actions to address identified privacy risks. Ideally, the individual completing the PIA should have the authority to direct mitigation steps, not just to recommend changes after the fact. A PIA that states risk and describes what will be done in the future to mitigate it is a statement of poor privacy policy implementation and of a hope to improve. A PIA stating that identified privacy risks were mitigated along the way demonstrates that privacy was built into the system and was not just a theoretical goal.
- Most important, identify which privacy, civil rights, and civil liberties policies must be developed to avoid, mitigate, or eliminate risk to data maintained in the system.

Stakeholders can share the PIA to engage the public, policymakers, and others in a dialogue about the system, thereby fostering greater public trust. Policies that result from the PIA can include:

- Enhanced security features, such as improved audit capability or enhanced physical security.
- Updated records retention schedule.
- Publication of the purpose statement and privacy policy on the agency Web site or in a state register.
- Audit procedures.
- Challenge processes for data that originates in other systems.

The PIA will ultimately serve as the first step in identifying the privacy implications and vulnerabilities of your information system. It is a road map for developing a thoughtful and comprehensive privacy policy to protect personal and confidential information and will serve the needs of your agency and the public.

X. Institutionalizing the PIA Process

Conducting a PIA at the state, local, and tribal levels is a best practice that should become a standard component of any strategic planning process aimed at automation and information sharing. As noted previously, the E-Government Act of 2002 requires federal agencies to conduct PIAs of new or significantly modified information systems. Few states have statutory requirements to conduct PIAs, either of new, significantly modified, or existing information systems. If your state is considering institutionalizing a PIA process, model legislation in Appendix C and a governor's executive order in Appendix D provide suggestions for such undertakings.

A. Social Media

State, local, and tribal entities are turning to social media sites both as a communications tool and as an open source of information to support law enforcement investigative activities. Conducting a PIA on the organization's process, procedures, and intended use of social media helps with the public understanding of the entity's process; determines, for law enforcement and the entity, as a whole, where the privacy risks exist; and also provides useful insights into the planning around the organization's presence on social media. Appendix F outlines resources, including guidance from federal agencies and the International Association of Chiefs of Police (IACP) Center for Social Media, to assist in the use of PIAs for the entity's social media process.

Federal PIA Example—DHS Conducts PIA, Results in Notice and Redress

The U.S. Department of Homeland Security (DHS), Customs and Border Protection (CBP), conducted a PIA of its Automated Commercial Environment (ACE) System, a program to monitor passage of commodities, materials, crew members, and passengers across U.S. borders.

As a result of the PIA process, participating truck carriers are asked to provide their drivers with notice regarding the collection and use of their information as well as how to seek redress if their records are inaccurate. CBP created a fact sheet to provide drivers with additional notice. See www.dhs.gov/xlibrary/assets/privacy/privacy_pia_cbp_aceitds.pdf.

Conclusion

As outlined in this guide, the consequences of inadequate or careless data protections are too severe for SLT justice entities to delay assessing the privacy implications and vulnerabilities of their information systems. News stories about agencies that failed to properly protect their data and that let personal and confidential information fall into the wrong hands are all too common. Do not let your entity make the headlines for the wrong reasons; perform a PIA to identify possible privacy risks associated with the entity's information sharing system.

I. Where to Turn for More Information

Once the PIA is complete, entities are encouraged to refer to resources for Stage 3—"Develop the Privacy Policy" in the Privacy Program Cycle for tools to assist in the policy development process. For more information on all of the privacy resources available for each stage of a Privacy Program Cycle, refer to DOJ's ***Global Privacy Resources***, available at www.it.ojp.gov/privacy.

For more information on the development of this and other Global privacy resources, as well as to request printed copies, please send the request via e-mail to GLOBAL@iir.com.

II. About Global

The PIA Guide was developed through a collaborative effort of the Global Privacy and Information Quality Working Group (GPIQWG) of the U.S. Department of Justice's (DOJ) Global Justice Information Sharing Initiative (Global). Global serves as a Federal Advisory Committee (FAC) and advises the U.S. Attorney General on justice information sharing and integration initiatives. Global promotes standards-based electronic information exchange to provide justice and public safety communities with timely, accurate, complete, and accessible information in a secure and trusted environment. For more information on Global, refer to: www.it.ojp.gov/global.

Global supports the initiatives of DOJ and aids Global member organizations and the people they serve through a series of important collaborative efforts. These include the

facilitation of Global working groups. GPIQWG is one of five Global working groups and is a cross-functional, multidisciplinary body composed of privacy and SLT and federal justice representatives covering critical topics such as intelligence, biometrics, information quality, privacy, civil rights, and civil liberties.

III. About GPIQWG

GPIQWG assists government entities, institutions, and other justice agencies in ensuring that PII is appropriately collected, used, maintained, and disseminated within evolving integrated justice information systems. For more information on GPIQWG, refer to www.it.ojp.gov/gpiqwg.

GPIQWG developed this guide and template as a practical hands-on tool to assist SLT justice entities in performing Privacy Impact Assessments. Through this effort, SLT entities can ensure that privacy risks are identified and policies can be developed to address these risks. To learn more about privacy-related resources developed by Global, refer to www.it.ojp.gov/privacy.

Appendix A—Privacy Impact Assessment Template

Instructions for Completing the Privacy Impact Assessment—PIA Template Column Headings

The following information is provided to assist individuals in performing the PIA.

Template Section—PIA questions are grouped into sections of related policy concepts that mirror the framework of the *Privacy, Civil Rights, and Civil Liberties Policy Development Template for State, Local, and Tribal Justice Entities* (SLT Policy Development Template), used to draft the entity privacy policy. Structuring the questions in this format prepares the practitioner performing the PIA for the next step, applying this information to the privacy policy.

PIA Questions—Pose questions for response or action.

Suggested Respondent(s)—General list of individuals (or roles) within the entity who are recommended to answer or contribute to the answer to the particular question. Other appropriate positions may be added or substituted as needed.

Entity Administrator: The chief executive officer or chief operations officer of the agency or organization. This could also be a department or division head over a particular organizational unit responsible for data collected and shared via an information exchange.

System Administrator: The chief information officer or other senior official responsible for overseeing the overall IT functions of an agency or organization.

Data Privacy Officer/Legal Counsel: The agency or organization privacy officer or attorney responsible for ensuring that the entity complies with all relevant privacy laws and policies. This should be the person who acts as the senior policy advisor on overall privacy policy, including legislative language, regulations, and other nonregulatory guidance related to or including privacy, confidentiality, or data security.

Technical/Systems Security Staff: The agency or organization staff person(s) responsible for implementing the technical enforcement of all relevant privacy and security policies (e.g., user authentication, access control, audit logs, firewalls, encryption).

Answer—The respondent(s) respond(s) to each question, as appropriate:

- Yes – Fully meets requirement
- No – Does not meet requirement
- Incomplete – Partially meets requirement
- N/A – Does not apply

Assessment of Risk—Make a judgment as to the likelihood, severity, and risk tolerance level of the privacy risk.[6] Recommended guidelines:

Likelihood that risk will occur

Remote: The risk probably will not occur because the risk would be difficult to realize, or there are solid means in place to limit the risk appropriately.

Possible: The risk has a chance of occurring, but it may be difficult or there are policies or procedures in place to help avoid the risk.

Likely: Because of conditions and capabilities, the risk is likely to occur.

Severity of identified risk

Low: The risk is manageable through planning and action, and the impacts generally are minimal.

Medium: The risk will be mitigated through planning and action. If it occurs, it will still have some impact on more important areas of concern.

High: The risk will have serious impacts; without extensive planning and action, its consequences would be severe.

Your tolerance for that risk

Avoidance: Avoidance is often used for risks that have the capacity for negative impact but have little known recourse. In privacy projects, a decision to avoid risks often means a decision not to let your agency put itself in a situation wherein it could incur the risk. Therefore, your decision would also be to avoid the cause of the risk.

Assume: The decision to assume a risk means accepting the risk as is and not implementing any policies or procedures to lessen it. This is often the decision in cases where the risk is so minimal and of such limited impact, should it occur, that the cost of implementing a mechanism to minimize or reduce it would be far greater than the agency's concern.

6 For more about risk assessment, see *Law Enforcement Tech Guide for Information Technology Security: How to Assess Risk and Establish Effective Policies*, prepared by SEARCH, The National Consortium for Justice Information and Statistics, and published by the Office of Community Oriented Policing Services, U.S. Department of Justice. Available at www.search.org/files/pdf/ITSecTechGuide.pdf.

Mitigate: This is the most common decision to make for identified risks: to implement policies, procedures, and other controls to limit the risk to an acceptable level.

Transfer: Transfer the responsibility for a system or the risk itself to another party that can better accept and deal with the risk and/or that has the resources necessary to properly mitigate the risk.

- In the Corrective Action/Remediation column, record the corrective action or recommendation that your initiative will take to mitigate the identified risk.
- In the Assessment of Risk column, record the priority level of the risk: either 1 (high priority), 2 (moderate priority), or 3 (lowest priority).

Corrective Action/Remediation/Location—If the answer to the PIA question is "No" or "Incomplete," then respond in the Corrective Action/Remediation column as to what steps will be taken to respond to this requirement and who will be responsible for taking the necessary action(s).

If the answer to the PIA question is "Yes," then respond in the Corrective Action/Remediation column as to where the necessary information can be located to be included or referenced in the entity's privacy, civil rights, and civil liberties policy.

PIA Cover Page

Information Sharing System or Exchange(s) Assessed:	
System Names:	
Purpose:	
Assessment Date(s):	
Organizations/Entities Involved:	Assessors (Entity Representatives):
Project Manager:	
Final PIA Submitted to:	
Date Submitted:	
Approved by:	
Approval Date:	

Template Section	PIA Questions	Suggested Respondent(s)
A. Purpose Specification	1. Is there a written mission statement for the entity?	Entity Administrator
	2. Is there a written purpose statement for collecting personally identifiable information (PII)? Include all types.	Entity Administrator Data Privacy Officer/ Legal Counsel
	3. Does the entity's mission statement support the purpose for collecting PII?	Entity Administrator Data Privacy Officer/ Legal Counsel
B. Policy Applicability and Legal Compliance	1. Does the entity have legal authority for collecting, creating, storing, accessing, receiving, and sharing or viewing data? If so, include citation(s), if applicable.	System Administrator OR Data Privacy Officer/ Legal Counsel
	2. Will all individuals with physical or logical access to the entity information be subject to the privacy policy?	System Administrator OR Data Privacy Officer/ Legal Counsel
	3. How does the entity plan to provide the privacy policy to personnel, participating users, and individual users (for example, in print, online)?	System Administrator
	4. Will the entity require all individuals with physical or logical access to acknowledge receipt of the policy and agree to comply with the policy? (In writing or online?)	System Administrator
	5. Will the entity require that individuals with physical or logical access and information-originating and user agencies be in compliance with all applicable constitutional and statutory laws protecting privacy, civil rights, and civil liberties in the gathering and collection, use, analysis, retention, destruction, sharing, disclosure, and dissemination of information? Note: These laws, statutes, and regulations will be cited in the privacy policy.	System Administrator OR Data Privacy Officer/ Legal Counsel
	6. Is a privacy notice required by law before data is collected, where appropriate (usually limited to health records)?	System Administrator OR Data Privacy Officer/ Legal Counsel

Answer (Yes, No, Incomplete, or N/A)	Assessment of Risk	Corrective Action/ Remediation/Location

Template Section	PIA Questions	Suggested Respondent(s)
C. Governance and Oversight	1. Is primary responsibility for the entity's overall operation—including the information systems, information collection and retention procedures, coordination of personnel, and enforcement of the privacy policy—assigned to one or more individuals?	System Administrator OR Data Privacy Officer/Legal Counsel
	2. Will the entity designate and train a privacy officer to handle reported errors and violations and oversee the implementation of privacy protections?	System Administrator
	3. Will the entity assign responsibility for ensuring that enforcement procedures and sanctions for noncompliance with the privacy policy are adequate and enforced?	Entity Administrator
D. Information	1. Has the entity identified the information it will seek, collect, retain, share, disclose, or disseminate?	System Administrator OR Data Privacy Officer/Legal Counsel
	2. Does the entity apply labels to information based on legal or policy restrictions or information sensitivity to indicate to authorized users how to handle the information?	Entity Administrator OR Data Privacy Officer/Legal Counsel OR Technical/ Systems Security Staff
	3. Does the entity categorize information based on its type (for example, tips and leads, suspicious activity reports, criminal history, intelligence information, case records, conditions of supervision, case progress), usability, and quality?	Entity Administrator OR Data Privacy Officer/Legal Counsel OR Technical/ Systems Security Staff
	4. Does the entity require certain basic descriptive information to be associated with each record, data set, or system of records containing PII (for example, source, originating entity, collection date, and contact information)?	System Administrator OR Data Privacy Officer/Legal Counsel OR Technical/ Systems Security Staff
	5. Is personal information obtained with the knowledge or consent of the data subject, if appropriate?	System Administrator

	Answer (Yes, No, Incomplete, or N/A)	Assessment of Risk	Corrective Action/ Remediation/Location

Template Section	PIA Questions	Suggested Respondent(s)
E. Acquiring and Receiving Information	1. Are there applicable state and federal constitutional provisions and statutes that govern or specify the techniques and methods the entity may employ when seeking and receiving information? Note: These laws, statutes, and regulations will be cited in the privacy policy.	System Administrator OR Data Privacy Officer/Legal Counsel
	2. Does the entity (if operational, conducting investigations) adhere to a policy regarding the investigative techniques to be followed when acquiring information (for example, an intrusion-level statement)?	System Administrator OR Data Privacy Officer/Legal Counsel
	3. Do agencies that access your entity's information and/or share information with your entity ensure that they will adhere to applicable law and policy?	System Administrator OR Data Privacy Officer/Legal Counsel
	4. Does the entity contract with commercial databases and, if so, does the entity ensure that the commercial database entity is in legal compliance in its information-gathering techniques?	System Administrator OR Data Privacy Officer/Legal Counsel
F. Information Quality Assurance	1. Has the entity established procedures and processes to ensure the quality (for example, accurate, complete, current, verifiable, and reliable) of the information it collects and maintains, including procedures for responding to alleged or suspected errors or deficiencies (for example, correction or destruction)?	System Administrator OR Data Privacy Officer/Legal Counsel
	2. Does the entity apply labels (or ensure that the originating agency has applied labels) to the information regarding its level of quality (for example, accurate, complete, current, verifiable, and reliable)?	System Administrator OR Data Privacy Officer/Legal Counsel OR Technical/ Systems Security Staff
	3. Does the entity review the quality of the information it originates to identify data that may be inaccurate or incomplete?	System Administrator OR Data Privacy Officer/Legal Counsel
	4. When information that is received from or provided to another agency is determined to be inaccurate or incomplete, does the entity notify the originating or recipient agency?	System Administrator OR Data Privacy Officer/Legal Counsel

Answer (Yes, No, Incomplete, or N/A)	Assessment of Risk	Corrective Action/ Remediation/Location

Template Section	PIA Questions	Suggested Respondent(s)
G. Collation and Analysis	1. Is there a policy stating the purpose for which information is analyzed and specifying who is authorized (position/title, credentials, etc.) to analyze information?	System Administrator OR Data Privacy Officer/ Legal Counsel
	2. Has the entity defined what information can be analyzed?	System Administrator OR Data Privacy Officer/ Legal Counsel
H. Merging Records	1. Does the entity identify who is authorized (position/title, credentials, clearance level[s], etc.) to merge records?	System Administrator OR Data Privacy Officer/ Legal Counsel OR Technical/Systems Security Staff
	2. Does the entity define matching criteria for merging information from multiple records allegedly about the same individual (e.g., sufficient identifying information beyond "name")?	System Administrator OR Data Privacy Officer/ Legal Counsel OR Technical/Systems Security Staff
	3. If the criteria specified above are not met, does the entity have a procedure for partial matches? Note: If the agency or exchange does not merge records that have partial matches, the policy should state this.	System Administrator OR Data Privacy Officer/ Legal Counsel OR Technical/Systems Security Staff

	Answer (Yes, No, Incomplete, or N/A)	Assessment of Risk	Corrective Action/ Remediation/Location

Template Section	PIA Questions	Suggested Respondent(s)
I. Sharing and Disclosure	1. Does the entity assign credentialed role-based levels of access for authorized users (for example, class of access and permissions to view, add, change, delete, or print)?	System Administrator OR Data Privacy Officer/ Legal Counsel OR Technical/Systems Security Staff
	2. Has the entity defined the conditions and credentials for access to and disclosure of records within the entity or in other governmental entities (for example, for law enforcement, public protection, public prosecution, public health, or justice purposes)?	System Administrator OR Data Privacy Officer/ Legal Counsel OR Technical/Systems Security Staff
	3. Are participating agencies that access information from your entity required to obtain approval from the originator of the information prior to further dissemination or to follow the disclosure laws applicable to the originating agency?	System Administrator OR Data Privacy Officer/ Legal Counsel
	4. Has the entity identified those laws or policies that specify when a record can be disclosed to a member of the public?	System Administrator OR Data Privacy Officer/ Legal Counsel
	5. Does the entity maintain an audit trail to document access to and disclosure of information retained by the entity (e.g., dissemination logs)?	System Administrator OR Data Privacy Officer/ Legal Counsel OR Technical/Systems Security Staff
	6. If release of information can be made only under exigent circumstances, are those circumstances described?	System Administrator OR Data Privacy Officer/ Legal Counsel
	7. Does the entity adhere to laws or policies for confirming the existence or nonexistence of information to persons or agencies that are not eligible to receive the information?	System Administrator OR Data Privacy Officer/ Legal Counsel

	Answer (Yes, No, Incomplete, or N/A)	Assessment of Risk	Corrective Action/ Remediation/Location

Template Section	PIA Questions	Suggested Respondent(s)
J. Redress **J.1 Disclosure**	**Disclosure** 1. If required by law or policy, has the entity established procedures for disclosing information to an individual about whom information has been gathered (for example, proof of identity, fingerprints)?	System Administrator OR Data Privacy Officer/ Legal Counsel
	2. Are there conditions under which an entity will not disclose information to an individual about whom information has been gathered? Note: The privacy policy will cite applicable legal authority for each stated basis for denial.	System Administrator OR Data Privacy Officer/ Legal Counsel
	3. If the entity did not originate the information and does not have the right to disclose it, are there circumstances in which the entity will either refer the individual to the agency originating the information or notify the originating agency of the request?	System Administrator OR Data Privacy Officer/ Legal Counsel
J.2. Corrections	**Corrections** 1. Has the entity established procedures for handling individuals' requests for correction involving information the entity has disclosed and can change because it originated the information?	System Administrator OR Data Privacy Officer/ Legal Counsel
J.3 Appeals	**Appeals** 1. If requests for disclosure or corrections are denied, does the entity have established procedures for appeal?	System Administrator OR Data Privacy Officer/ Legal Counsel

	Answer (Yes, No, Incomplete, or N/A)	Assessment of Risk	Corrective Action/ Remediation/Location

Template Section	PIA Questions	Suggested Respondent(s)
K. Security Safeguards	1. Does the agency or exchange have a designated security officer?	Entity Administrator OR Data Privacy Officer/Legal Counsel OR Technical/ Systems Security Staff
	2. Does the entity have physical, procedural, and technical safeguards for ensuring the security of its data? Note: The privacy policy will describe how information will be protected from unauthorized access, modification, theft, or sabotage (whether internal or external) resulting from natural or human-caused disasters or intrusions with, for example, procedures, practices, system protocols, use of software, information technology tools, and physical security measures.	Entity Administrator OR Data Privacy Officer/Legal Counsel OR Technical/ Systems Security Staff
	3. Is information stored in a secure format and a secure environment?	Entity Administrator OR Data Privacy Officer/Legal Counsel OR Technical/ Systems Security Staff
	4. Does the entity utilize watch logs to maintain audit trails of requested and disseminated information, and do logs identify the user initiating the query?	Entity Administrator OR Data Privacy Officer/Legal Counsel OR Technical/ Systems Security Staff
	5. Does the entity have established procedures for adhering to data breach notification laws or policies?	Entity Administrator OR Data Privacy Officer/Legal Counsel OR Technical/ Systems Security Staff
L. Information Retention and Destruction	1. Does the entity have a records retention and destruction policy (including methods for removing or destroying information)?	System Administrator OR Data Privacy Officer/Legal Counsel
	2. Does the entity have a review schedule for validating or purging information?	System Administrator OR Data Privacy Officer/Legal Counsel
	3. Will there be a periodic review of collected data to make sure they are still needed? If so, include the review schedule.	System Administrator

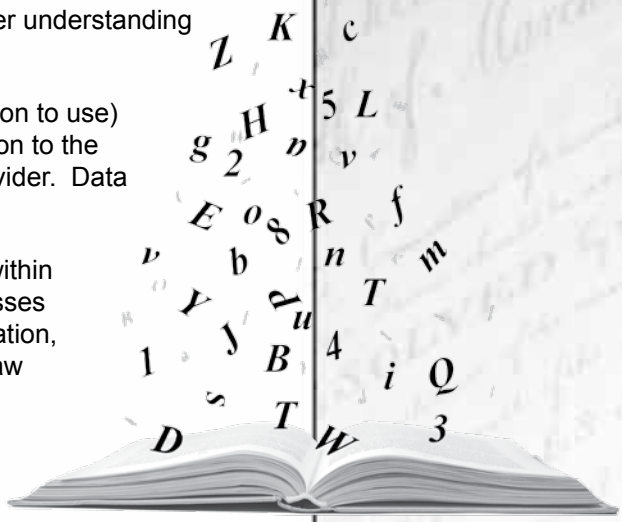
Answer (Yes, No, Incomplete, or N/A)	Assessment of Risk	Corrective Action/ Remediation/Location

Template Section	PIA Questions	Suggested Respondent(s)
M. Accountability and Enforcement **M.1 Information System Transparency**	**Information System Transparency** 1. Does the entity have a point of contact (position/title) for handling inquiries or complaints?	System Administrator OR Data Privacy Officer/ Legal Counsel
	2. Will the privacy policy be available on the entity's public Web site?	System Administrator OR Data Privacy Officer/ Legal Counsel
M.2 Accountability	**Accountability** 1. Are there procedures and practices the entity follows to enable evaluation of user compliance with system requirements and applicable law, as well as its privacy policy, when established?	System Administrator OR Data Privacy Officer/Legal Counsel OR Technical/ Systems Security Staff
	2. Is there an established mechanism for personnel to report errors and suspected or confirmed violations of policies related to protected information?	System Administrator OR Data Privacy Officer/ Legal Counsel
M.3 Enforcement	**Enforcement** 1. Has the entity established procedures for enforcement (sanctions) if an agency or authorized user is suspected of being or has been found to be in noncompliance with the laws and policies, including the entity's privacy policy, when established?	System Administrator OR Data Privacy Officer/ Legal Counsel
N. Training	1. Will the entity require any individual having physical or logical access to entity information to participate in training programs regarding the implementation of and adherence to the privacy policy?	System Administrator OR Data Privacy Officer/ Legal Counsel
	2. Will the entity's privacy training program cover the purpose of the policy, substance and intent of the provisions of the policy, impact of infractions, and possible penalties for violations?	System Administrator OR Data Privacy Officer/ Legal Counsel

Answer (Yes, No, Incomplete, or N/A)	Assessment of Risk	Corrective Action/ Remediation/Location

Appendix B—Glossary of Terms and Definitions

The following list of primary terms and definitions is provided for further understanding of this topic.



Access—Data access is being able to get to (usually having permission to use) particular data on a computer. Web access means having a connection to the World Wide Web through an access provider or an online service provider. Data access is usually specified as read-only and read/write access.

With regard to the Information Sharing Environment (ISE) (see term within this glossary), access refers to the business rules, means, and processes by and through which ISE participants obtain terrorism-related information, to include homeland security information, terrorism information, and law enforcement information acquired in the first instance by another ISE participant.

Access Control—The mechanisms for limiting access to certain information based on a user's identity and membership in various predefined groups. Access control can be mandatory, discretionary, or role-based.

Acquisition—The means by which an Information Sharing Environment (ISE) (see term within this glossary) participant obtains information through the exercise of its authorities; for example, through human intelligence collection or from a foreign partner. For the purposes of this definition, acquisition does not refer to the obtaining of information widely available to other ISE participants through, for example, news reports or to the obtaining of information shared with them by another ISE participant who originally acquired the information.

Agency—A participating agency that accesses, contributes, and/or shares information in the [name of entity]'s justice information system.

Audit Trail—A generic term for recording (logging) a sequence of activities. In computer and network contexts, an audit trail tracks the sequence of activities on a system, such as user log-ins and log-outs. More expansive audit trail mechanisms would record each user's activity in detail—what commands were issued to the system, what records and files were accessed or modified, etc.

Audit trails are a fundamental part of computer security, used to trace (albeit usually retrospectively) unauthorized users and uses. They can also be used to assist with information recovery in the event of a system failure.

Authentication—The process of validating the credentials of a person, computer process, or device. Authentication requires that the person, process, or device making the request provide a credential that proves it is what or who it says it is. Common forms of credentials are digital certificates, digital signatures, smart cards, biometrics data, and a combination of user names and passwords. See Biometrics.

Authorization—The process of granting a person, computer process, or device access to certain information, services, or functionality. Authorization is derived from the identity of the person, computer process, or device requesting access that is verified through authentication. See Authentication.

Biometrics—Biometrics methods can be divided into two categories: physiological and behavioral. Implementations of the former include face, eye (retina or iris), finger (fingertip, thumb, finger length, or pattern), palm (print or topography), and hand geometry. The latter includes voiceprints and handwritten signatures.

Center—Refers to the [name of entity] and all participating state entities of the [name of entity].

Civil Liberties—Fundamental individual rights, such as freedom of speech, press, or religion; due process of law; and other limitations on the power of the government to restrain or dictate the actions of individuals. They are the freedoms that are guaranteed by the Bill of Rights—the first ten Amendments to the Constitution of the United States. Civil liberties offer protection to individuals from improper government action and arbitrary governmental interference. Generally, the term “civil rights” involves positive (or affirmative) government action, while the term “civil liberties” involves restrictions on government.

Civil Rights—The term “civil rights” is used to imply that the state has a role in ensuring that all citizens have equal protection under the law and equal opportunity to exercise the privileges of citizenship regardless of race, religion, gender, or other characteristics unrelated to the worth of the individual. Civil rights are, therefore, obligations imposed on government to promote equality. Specifically, they are the rights to personal liberty guaranteed to all United States citizens by the Thirteenth and Fourteenth Amendments and by acts of Congress.

Computer Security—The protection of information assets through the use of technology, processes, and training.

Confidentiality—Closely related to privacy but not identical. It refers to the obligations of individuals and institutions to use information under their control appropriately once it has been disclosed to them. One observes rules of confidentiality out of respect for and to protect and preserve the privacy of others. See also Privacy.

Credentials—Information that includes identification and proof of identification that is used to gain access to local and network resources. Examples of credentials are user names, passwords, smart cards, and certificates.

Criminal Intelligence Information—Information deemed relevant to the identification of and the criminal activity engaged in by an individual who or organization that is reasonably suspected of involvement in criminal activity. Criminal intelligence records are maintained in a criminal intelligence system according to 28 CFR Part 23.

Data—Inert symbols, signs, descriptions, or measures; elements of information.

Data Breach—The unintentional release of secure information to an untrusted environment. This may include incidents such as theft or loss of digital media—including computer tapes, hard drives, or laptop computers containing such media—upon which such information is stored unencrypted; posting such information on the World Wide Web or on a computer otherwise accessible from the Internet without proper information security precautions; transfer of such information to a system that is not completely open but is not appropriately or formally accredited for security at the approved level, such as unencrypted e-mail; or transfer of such information to the information systems of a possibly hostile entity or environment where it may be exposed to more intensive decryption techniques.

Data Protection—Encompasses the range of legal, regulatory, and institutional mechanisms that guide the collection, use, protection, and disclosure of information.

Disclosure—The release, transfer, provision of access to, sharing, publication, or divulging of personal information in any manner—electronic, verbal, or in writing—to an individual, entity, or organization outside the entity that collected it. Disclosure is an aspect of privacy, focusing on information which may be available only to certain people for certain purposes but which is not available to everyone.

Electronically Maintained—Information stored by a computer or on any electronic medium from which the information may be retrieved by a computer, such as electronic memory chips, magnetic tape, magnetic disk, or compact disc optical media.

Electronically Transmitted—Information exchanged with a computer using electronic media, such as the movement of information from one location to another by magnetic or optical media, or transmission over the Internet, intranet, extranet, leased lines, dial-up lines, private networks, telephone voice response, or faxback systems. It does not include faxes, telephone calls, video teleconferencing, or messages left on voicemail.

Entity—The [name of entity] that is the subject and owner of the privacy policy.

Fair Information Principles—The Fair Information Principles (FIPs) are contained within the Organisation for Economic Co-operation and Development's (OECD) *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*. These were developed around commercial transactions and the transborder exchange of information; however, they do provide a straightforward description of underlying privacy and information exchange principles and a simple framework for the legal analysis that needs to be done with regard to privacy in integrated justice systems. Some of the individual principles may not apply in all instances of an integrated justice system.

The eight FIPs are:

- Collection Limitation Principle
- Data Quality Principle
- Purpose Specification Principle
- Use Limitation Principle
- Security Safeguards Principle
- Openness Principle
- Individual Participation Principle
- Accountability Principle

Firewall—A security solution that segregates one portion of a network from another portion, allowing only authorized network traffic to pass through according to traffic-filtering rules.

General Information or Data—Information that may include records, documents, or files pertaining to law enforcement operations, such as computer-aided dispatch (CAD) data, incident data, and management information. Information that is maintained in a records

management system, CAD system, etc., for statistical/retrieval purposes. Information may be either resolved or unresolved. The record is maintained according to statute, rule, or policy.

Homeland Security Information—As defined in Section 892(f)(1) of the Homeland Security Act of 2002 and codified at 6 U.S.C. § 482(f)(1), homeland security information means any information possessed by a federal, state, or local entity that (a) relates to a threat of terrorist activity; (b) relates to the ability to prevent, interdict, or disrupt terrorist activity; (c) would improve the identification or investigation of a suspected terrorist or terrorist organization; or (d) would improve the response to a terrorist act.

Identification—A process whereby a real-world entity is recognized and its identity established. Identity is operationalized in the abstract world of information systems as a set of information about an entity that uniquely differentiates it from other similar entities. The set of information may be as small as a single code, specifically designed as an identifier, or a collection of data, such as a given and family name, a date of birth, and an address. An organization's identification process consists of the acquisition of the relevant identifying information.

Individual Responsibility—Because a privacy notice is not self-implementing, an individual within an organization's structure also must be assigned responsibility for enacting and implementing the notice.

Information—Includes any data about people, organizations, events, incidents, or objects, regardless of the medium in which it exists. Information received by law enforcement entities can be categorized into four general areas: general data, including investigative information; tips and leads data; suspicious activity reports; and criminal intelligence information.

Information Quality—Refers to various aspects of the information and the accuracy and validity of the actual values of the data, data structure, and database/data repository design. Traditionally, the basic elements of information quality have been identified as accuracy, completeness, currency, reliability, and context/meaning. Today, information quality is being more fully described in multidimensional models, expanding conventional views of the topic to include considerations of accessibility, security, and privacy.

Information Sharing Environment (ISE)—In accordance with Section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), as amended, the ISE is a conceptual framework composed of the policies, procedures, and technologies linking the resources (people, systems, databases, and information) of state, local, and tribal (SLT) entities; federal agencies; and the private sector to facilitate terrorism-related information sharing, access, and collaboration. Consistent with Presidential Guideline 5, the U.S. Attorney General, the U.S. Department of Justice (DOJ), and the Director of National Intelligence (DNI)—in coordination with the Program Manager for the ISE (PM-ISE) and the heads of federal departments and agencies that possess or use intelligence or other terrorism-related information—developed privacy guidelines for the ISE, titled *Guidelines to Ensure That the Information Privacy and Other Legal Rights of Americans Are Protected in the Development and Use of the Information Sharing Environment* (ISE Privacy Guidelines). The ISE Privacy Guidelines describe the means by which federal departments and agencies participating in the ISE will protect privacy and civil liberties in the development and operation of the ISE.

Information Sharing Environment (ISE) Suspicious Activity Report (SAR) (ISE-SAR)—A SAR that has been determined, pursuant to a two-step process established in the ISE-SAR Functional Standard, to have a potential terrorism nexus (i.e., to be reasonably indicative of criminal activity associated with terrorism). Refer to Information Sharing Environment (ISE) within this glossary.

Intelligence-Led Policing (ILP)—A process for enhancing law enforcement entity effectiveness toward reducing crimes, protecting community assets, and preparing for responses. ILP provides law enforcement entities with an organizational framework to gather and use multisource information and intelligence to make timely and targeted strategic, operational, and tactical decisions.

Invasion of Privacy—Intrusion on one's solitude or into one's private affairs, public disclosure of embarrassing private information, publicity that puts one in a false light to the public, or appropriation of one's name or picture for personal or commercial advantage. See also Right to Privacy.

Law—As used by this policy, "law" includes any local, state, or federal constitution, statute, ordinance, regulation, executive order, policy, or court rule, decision, or order as construed by appropriate local, state, or federal officials or entities.

Law Enforcement Information—For purposes of the Information Sharing Environment (ISE) (see term within this glossary), law enforcement information means any information obtained by or of interest to a law enforcement entity or official that is both (a) related to terrorism or the security of our homeland and (b) relevant to a law enforcement mission, including but not limited to information pertaining to an actual or potential criminal, civil, or administrative investigation or a foreign intelligence, counterintelligence, or counterterrorism investigation; assessment of or response to criminal threats and vulnerabilities; the existence, organization, capabilities, plans, intentions, vulnerabilities, means, methods, or activities of individuals or groups involved or suspected of involvement in criminal or unlawful conduct or assisting or associated with criminal or unlawful conduct; the existence, identification, detection, prevention, interdiction, or disruption of or response to criminal acts and violations of the law; identification, apprehension, prosecution, release, detention, adjudication, supervision, or rehabilitation of accused persons or criminal offenders; and victim/witness assistance.

Lawful Permanent Resident—A foreign national who has been granted the privilege of permanently living and working in the United States.

Least Privilege Administration—A recommended security practice in which every user is provided with only the minimum privileges needed to accomplish the tasks he or she is authorized to perform.

Logs—A necessary part of an adequate security system because they are needed to ensure that data is properly tracked and that only authorized individuals are getting access to the data. See also Audit Trail.

Maintenance of Information—Applies to all forms of information storage. This includes electronic systems (for example, databases) and nonelectronic storage systems (for example, filing cabinets). To meet access requirements, an organization is not required to create new systems to maintain information or to maintain information beyond a time when it no longer serves an organization's purpose.

Metadata—In its simplest form, metadata is information (data) about information; specifically, information about a particular aspect of the collected information. An item of metadata may describe an individual content item or a collection of content items. Metadata is used to facilitate the understanding, use, and management of information. The metadata required for this will vary based on the type of information and the context of use.

Need to Know—As a result of jurisdictional, organizational, or operational necessities, access to sensitive information or intelligence is necessary for the conduct of an individual's official duties as part of an organization that has a right to know the information in the performance of a law enforcement, homeland security, or counterterrorism activity, such as to further an investigation or meet another law enforcement requirement.

Nonrepudiation—A technique used to ensure that someone performing an action on a computer cannot falsely deny that he or she performed that action. Nonrepudiation provides undeniable proof that a user took a specific action, such as transferring money, authorizing a purchase, or sending a message.

Originating Entity—The entity or organizational entity that documents information or data, including source entities that document SAR (and, when authorized, ISE-SAR) information that is collected by an entity. Refer to Information Sharing Environment (ISE) within this glossary.

Participating Entity—An organizational entity that is authorized to access or receive and use entity information and/or intelligence databases and resources for lawful purposes through its authorized individual users.

Permissions—Authorization to perform operations associated with a specific shared resource, such as a file, directory, or printer. Permissions must be granted by the system administrator to individual user accounts or administrative groups.

Personal Data—Any information that relates to an identifiable individual (or data subject). See also Personally Identifiable Information.

Personal Information—Information that can be used, either alone or in combination with other information, to identify individual subjects suspected of engaging in criminal activity, including terrorism. See also Personally Identifiable Information.

Personally Identifiable Information—One or more pieces of information that, when considered together or in the context of how the information is presented or gathered, are sufficient to specify a unique individual. The pieces of information can be:

- Personal characteristics (such as height, weight, gender, sexual orientation, date of birth, age, hair color, eye color, race, ethnicity, scars, tattoos, gang affiliation, religious affiliation, place of birth, mother's maiden name, distinguishing features, and biometrics information, such as fingerprints, DNA, and retinal scans).

- A unique set of numbers or characters assigned to a specific individual (including name, address, phone number, social security number, e-mail address, driver's license number, financial account or credit card number and associated PIN number, Integrated Automated Fingerprint Identification System [IAFIS] identifier, or booking or detention system number).

- Descriptions of event(s) or points in time (for example, information in documents such as police reports, arrest reports, and medical records).

- Descriptions of location(s) or place(s) (including geographic information systems [GIS] locations, electronic bracelet monitoring information, etc.).

Persons—Executive Order 12333 defines "United States persons" as United States citizens, aliens known by the intelligence entity concerned to be permanent resident aliens, an unincorporated association substantially composed of United States citizens or permanent resident aliens, or a corporation incorporated in the United States, except for a corporation directed and controlled by a foreign government or governments. For the Intelligence Community and for domestic law enforcement entities, "persons" means United States citizens and lawful permanent residents.

Privacy—Individuals' interests in preventing the inappropriate collection, use, and release of personal information. Privacy interests include privacy of personal behavior, privacy of personal communications, and privacy of personal data. Other definitions of privacy include the capacity to be physically left alone (solitude); to be free from physical interference, threat, or unwanted touching (assault, battery); or to avoid being seen or overheard in particular contexts.

Privacy Policy—A printed, published statement that articulates the policy position of an organization on how it handles the personal information that it gathers and uses in the normal course of business. The policy should include information relating to the processes of information collection, analysis, maintenance, dissemination, and access. The purpose of the privacy policy is to articulate that the entity will adhere to those legal requirements and entity policy determinations that enable gathering and sharing of information to occur in a manner that protects personal privacy interests. A well-developed and implemented privacy policy uses justice entity resources wisely and effectively; protects the entity, the individual, and the public; and promotes public trust.

Privacy Protection—A process of maximizing the protection of privacy, civil rights, and civil liberties when collecting and sharing information in the process of protecting public safety and public health.

Protected Information—Personal data about individuals that is subject to information privacy or other legal protections by law, including the U.S. Constitution and the [insert name of state] Constitution; applicable federal statutes and regulations, such as civil rights laws and 28 CFR Part 12; applicable state and tribal constitutions; and applicable state, local, and tribal laws and ordinances. Protection may also be extended to organizations by center policy or state, local, or tribal law.

Public—Public includes:

- Any person and any for-profit or nonprofit entity, organization, or association.
- Any governmental entity for which there is no existing specific law authorizing access to the entity's information.
- Media organizations.
- Entities that seek, receive, or disseminate information for whatever reason, regardless of whether it is done with the intent of making a profit, and without distinction as to the nature or intent of those requesting information from the entity or participating entity.

Public does not include:

- Employees of the entity or participating entity.
- People or entities, private or governmental, which assist the entity in the operation of the justice information system.
- Public entities whose authority to access information gathered and retained by the entity is specified in law.

Public Access—Relates to what information can be seen by the public; that is, information whose availability is not subject to privacy interests or rights.

Record—Any item, collection, or grouping of information that includes personally identifiable information and is maintained, collected, used, or disseminated by or for the collecting entity or organization.

Redress—Laws, policies, and procedures that address public entity responsibilities with regard to access/disclosure and correction of information and the handling of complaints from persons regarding protected information about them which is under the entity's control and which is exempt from disclosure and not disclosed to the individual to whom the information pertains.

Repudiation—The ability of a user to deny having performed an action that other parties cannot prove otherwise. For example, a user who deleted a file can successfully deny doing so if no mechanism (such as audit files) can contradict that claim.

Retention—Refer to Storage.

Right to Know—Based on having legal authority or responsibility or pursuant to an authorized agreement, an entity or organization is authorized to access sensitive information and intelligence in the performance of a law enforcement, homeland security, or counterterrorism activity.

Right to Privacy—The right to be left alone, in the absence of some reasonable public interest in gathering, retaining, and sharing information about a person's activities. Invasion of the right to privacy can be the basis for a lawsuit for damages against the person or entity violating a person's privacy.

Role-Based Access—A type of access authorization that uses roles to determine access rights and privileges. A role is a symbolic category of users that share the same security privilege.

Security—The range of administrative, technical, and physical business practices and mechanisms that aim to preserve privacy and confidentiality by restricting information access to authorized users for authorized purposes. Computer and communications security efforts also have the goal of ensuring the accuracy and timely availability of data for the legitimate user set, as well as promoting failure resistance in the electronic systems overall.

Source Entity—The entity or organizational entity that originates SAR (and, when authorized, ISE-SAR) information. See Information Sharing Environment (ISE) Suspicious Activity Report (ISE-SAR) within this glossary.

Storage—The place in a computer where data is held in an electromagnetic or optical form for access by a computer processor. There are two general usages:

Storage is frequently used to mean the devices and data connected to the computer through input/output operations—that is, hard disk and tape systems and other forms of storage that do not include computer memory and other in-computer storage. This is probably the most common meaning in the IT industry.

In a more formal usage, storage has been divided into (1) primary storage, which holds data in memory (sometimes called random access memory, or RAM) and other "built-in" devices such as the processor's L1 cache, and (2) secondary storage, which holds data on hard disks, tapes, and other devices requiring input/output operations.

Primary storage is much faster to access than secondary storage because of the proximity of the storage to the processor or because of the nature of the storage devices. On the other hand, secondary storage can hold much more data than primary storage.

With regard to the Information Sharing Environment (ISE), storage (or retention) refers to the storage and safeguarding of terrorism-related information—including homeland security information, terrorism information, and law enforcement information relating to terrorism or the security of our homeland—by both the originator of the information and any recipient of the information.

Suspicious Activity—Defined in the ISE-SAR Functional Standard (Version 1.5) as "observed behavior reasonably indicative of preoperational planning related to terrorism or other criminal activity." Examples of suspicious activity include surveillance, photography of sensitive infrastructure facilities, site breach or physical intrusion, cyberattacks, testing of security, etc.

Suspicious Activity Report (SAR)—Official documentation of observed behavior reasonably indicative of preoperational planning related to terrorism or other criminal activity. Suspicious activity report (SAR) information offers a standardized means for feeding information repositories or data analysis tools. Patterns identified during SAR information analysis may be investigated in coordination with the reporting entity and, if applicable, a state or regional entity. SAR information is not intended to be used to track or record ongoing enforcement, intelligence, or investigatory activities, nor is it designed to support interentity calls for service.

Terrorism Information—Consistent with Section 1016(a)(4) of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), all information relating to (a) the existence, organization, capabilities, plans, intentions, vulnerabilities, means of finance or materials support, or activities of foreign **or** international terrorist groups or individuals **or** of domestic groups **or** individuals involved in transnational terrorism; (b) threats posed by such groups or individuals to the United States, United States persons, or United States interests or to those interests of other nations; (c) communications of or by such groups or individuals; or (d) other groups or individuals reasonably believed to be assisting or associated with such groups or individuals.

Terrorism-Related Information—In accordance with the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), as amended by the 9/11 Commission Act (August 3, 2007, P.L. 110-53), the ISE facilitates the sharing of terrorism and homeland security information, as defined in IRTPA Section 1016(a)(5) and the Homeland Security Act 892(f)(1) (6 U.S.C. § 482(f)(1)). See also *Information Sharing Environment Implementation Plan* (November 2006) and Presidential Guidelines 2 and 3 (the ISE will facilitate the sharing of "terrorism information," as defined in the IRTPA, as well as the following categories of information to the extent that they do not otherwise constitute "terrorism information": (1) homeland security information as defined in Section 892(f)(1) of the Homeland Security Act of 2002 (6 U.S.C. § 482(f)(1)); and (2) law enforcement information relating to terrorism or the security of our homeland). Such additional information may include intelligence information.

Weapons of mass destruction (WMD) information was defined and included in the definition of "terrorism information" by P.L. 110-53.

Tips and Leads Information or Data—Generally information or uncorroborated reports generated from inside or outside a law enforcement entity that allege or indicate some form of possible criminal activity. Tips and leads are sometimes referred to as suspicious incident report (SIR), suspicious activity report (SAR), and/or field interview report (FIR) information. However, SAR information should be viewed, at most, as a subcategory of tips or leads data. Tips and leads information does not include incidents that do not have a criminal offense attached or indicated, criminal history records, or CAD data. Tips and leads information should be maintained in a secure system, similar to data that rises to the level of reasonable suspicion.

A tip or lead can come from a variety of sources, including, but not limited to, the public, field interview reports, and anonymous or confidential sources. This information may be based on mere suspicion or on a level of suspicion that is less than "reasonable suspicion" and, without further information or analysis, it is unknown whether the information is accurate or useful. Tips and leads information falls between being of little or no use to law enforcement and being extremely valuable, depending on the availability of time and resources to determine its meaning.

Tribal (entity/nation/government)—Pertaining to a domestic Native American government recognized by the U.S. Department of the Interior as a federally recognized tribe.

User—An individual representing a participating entity who is authorized to access or receive and use an entity's information and intelligence databases and resources for lawful purposes.

Appendix C—Model Legislation

Section 1.100 Purpose

To ensure that all criminal justice data information systems developed, procured, or significantly modified minimize the risk of inappropriate impacts on the privacy of individuals, the "Data System Privacy Review Act" is enacted.

Section 1.200 Definitions

a. "Criminal justice agency" has the meaning given provided in Section **[insert citation to appropriate state law]** and includes courts.

b. "Information system" includes any technology system or project that collects, maintains, or disseminates personally identifiable data.

c. "Personally identifiable data" means data from which an individual human being can be uniquely identified including but not limited to:

   1. First and last name
   2. Physical address
   3. E-mail address
   4. Telephone number
   5. Social security number
   6. Credit card information
   7. Bank account information
   8. Any combination of personal information that could be used to determine an individual's identity

d. "Privacy Impact Assessment" or "assessment" means answers to a series of questions approved by **[insert authority]** to evaluate how personally identifiable information is collected, stored, protected, shared, and managed by an electronic information system or online collections application.

Section 1.300 General Provisions

a. A criminal justice agency or court developing, procuring, or significantly modifying an existing information data system containing personally identifiable information shall complete a Privacy Impact Assessment authorized by **[insert authority]** before the system is implemented.

b. Completed assessments shall be posted on the criminal justice agency's Web site and maintained in the agency's principal office for four years.

c. Completed assessments shall be submitted to **[insert authority; e.g., chief information officer, chief privacy officer, attorney general's office]** for review and approval.

d. The **[insert authority]** shall report annually on January 15 to the Legislature all of the assessment completed in the prior year.

Section 1.400 Penalties

a. Agencies or courts failing to complete and submit a completed assessment in a timely manner may forfeit current and future funding for information technology systems.

Criminal justice agencies and system proponents could also encourage adoption of the following executive order (see Appendix D) by their state's governor.

Appendix D—Sample Executive Order

Note: The authors of this PIA Guide acknowledge that the following sample executive order may require modification for use by local (county, city) or tribal governments, since each has its own unique political structure and system of government. Also, the language may be customized as a resolution to reflect an entity's commitment to support privacy protections, such as through the completion of a PIA and development and implementation of an entity privacy policy, as opposed to an official order.

Improving Data Protection and Security by State Agencies

I, GOVERNOR _____ OF THE STATE OF _____, by virtue of the authority vested in me by the Constitution and applicable laws, do hereby issue this executive order:

WHEREAS, _____'s state agencies are the data stewards of personally identifiable information about its citizens in their possession and have a duty to protect that data from misuse, and appropriate management of sensitive information, including social security numbers, driver's license numbers, financial account numbers, and other similar sensitive personal information, respects the privacy of those individuals associated with that data;

WHEREAS, *sensitive information that is not adequately protected can cause individuals to suffer a variety of consequences, including invasion of privacy, personal embarrassment, stalking, harassment, identity theft, or other criminal misuses of their data*;

WHEREAS, identity theft costs our nation's citizens and businesses billions of dollars in losses each year, and misuse of sensitive data can also place individuals at risk for harassment, stalking, and other criminal acts;

NOW THEREFORE, I hereby order that:

1. The state's Chief Information Officer will be responsible for coordinating the implementation of improved privacy measures.

2. Within 90 days, the state's Chief Information Office shall develop and disseminate

a Privacy Impact Assessment (PIA) Directive for use by state agencies for all new or significantly modified information data systems. The Directive will address what information is to be collected, why the information is being collected, intended use of the information, with whom the information will be shared, what opportunities individuals have to decline to provide information or to consent to particular uses of the information (other than required or authorized uses), how individuals can grant consent, and how the information will be secured.

3. Within one year, all state agency heads shall conduct Privacy Impact Assessments on all existing systems that maintain personally identifiable information to include names and addresses, social security numbers, driver's license numbers, and financial institution account information of more than (10,000) individuals.

4. Prior to requesting any state funds to develop, procure, or significantly modify a data system, state agency heads shall conduct a Privacy Impact Assessment.

5. Completed Privacy Impact Assessments shall be prominently posted on a state agency's Web site for at least two years.

Pursuant to **[insert cite]**, this executive order will be effective until **[insert date]**.

Appendix E—Office of Management and Budget Memorandum

(OMB M-03-022), OMB Guidance for Implementing the Privacy Provision of the E-Government Act of 2002

In general, PIAs are required to be performed and updated as necessary when a system change creates new privacy risks. For example:

a. **Conversions**—when converting paper-based records to electronic systems;

b. **Anonymous to Non-Anonymous**—when functions applied to an existing information collection change anonymous information into information in identifiable form;

c. **Significant System Management Changes**—when new uses of an existing IT system, including application of new technologies, significantly change how information in identifiable form is managed in the system:

- For example, when an agency employs new relational database technologies or Web-based processing to access multiple data stores; such additions could create a more open environment and avenues for exposure of data that previously did not exist.

d. **Significant Merging**—when agencies adopt or alter business processes so that government databases holding information in identifiable form are merged, centralized, matched with other databases or otherwise significantly manipulated:

- For example, when databases are merged to create one central source of information; such a link may aggregate data in ways that create privacy concerns not previously at issue.

e. **New Public Access**—when user-authenticating technology (e.g., password, digital certificate, biometric) is newly applied to an electronic information system accessed by members of the public;

f. **Commercial Sources**—when agencies systematically incorporate into existing information systems databases of information in identifiable form purchased or obtained from commercial or public sources. (Merely querying such a source on an ad hoc basis using existing technology does not trigger the PIA requirement);

g. **New Interagency Uses**—when agencies work together on shared functions involving significant new uses or exchanges of information in identifiable form, such as the cross-cutting E-Government initiatives; in such cases, the lead agency should prepare the PIA;

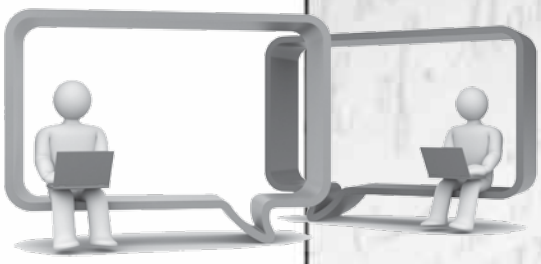
- For example, the Department of Health and Human Services, the lead agency for the Administration's Public Health Line of Business (LOB) Initiative, is spearheading work with several agencies to define requirements for integration of processes and accompanying information exchanges. HHS would thus prepare the PIA to ensure that all privacy issues are effectively managed throughout the development of this cross-agency IT investment.

h. **Internal Flow or Collection**—when alteration of a business process results in significant new uses or disclosures of information or incorporation into the system of additional items of information in identifiable form:

- For example, agencies that participate in E-Gov initiatives could see major changes in how they conduct business internally or collect information, as a result of new business processes or E-Gov requirements. In most cases the focus will be on integration of common processes and supporting data. Any business change that results in substantial new requirements for information in identifiable form could warrant examination of privacy issues.

i. **Alteration in Character of Data**—when new information in identifiable form added to a collection raises the risks to personal privacy (for example, the addition of health or financial information).

Appendix F—Social Media



In response to the increased use of social media Web sites (such as Facebook, Twitter, LinkedIn, YouTube, and blogs), federal, state, local, and tribal agencies and law enforcement organizations have embraced social media tools for various purposes, including:

- **Communications**—increasing public awareness and outreach to and engagement with constituents and fostering greater transparency and connections within communities.
- **Networking**—connecting with other law enforcement organizations and associations.
- **Investigations**—gathering open source information or evidence to support a legitimate law enforcement purpose.
- **Notifications**—providing time-sensitive notifications to the public.

From a privacy perspective, the general public may not differentiate between an organization's various uses of social media. It is in the interest of federal, state, local, and tribal organizations to proactively notify the public and their specific constituent bodies of the organization's intended uses of social media tools.

Guidance on Privacy Impact Assessments for Social Networking

In June 2010, the Office of Management and Budget (OMB) issued Memorandum 10-23, *Guidance for Agency Use of Third-Party Websites and Applications* (June 25, 2010), which updates the guidance of OMB Memorandum 03-22 (*OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002* (September 30, 2003)) regarding Privacy Impact Assessments (PIA). OMB Memorandum 10-23 directs federal agencies planning the use of third-party social media sites and applications to prepare an adapted PIA whenever an agency's use of a third-party Web site or application makes personally identifiable information (PII) available to the agency. In December 2011, OMB, in collaboration with the Privacy Committee of the federal Chief Information Officers (CIO) Council, issued additional guidance and a model template PIA for use by federal agencies engaging in the use of social media.

Both OMB Memorandum 10-23 and the December 2011 OMB Model PIA guidance recommend addressing the following questions when developing a PIA for social media:

i. The specific purpose of the agency's use of the social networking Web site or application.

ii. Any PII that is likely to become available to the agency through public use of the social networking Web site or application.

iii. The agency's intended or expected use of PII.

iv. With whom the agency will share PII.

v. Whether and how the agency will maintain/retain PII and for how long.

vi. How the agency will secure PII that it uses or maintains.

vii. How safeguards will be used to prevent unauthorized uses of PII.

viii. What other privacy risks exist and how the agency will mitigate those risks.

The adapted PIA should also address whether the agency's activities will affect legal and regulatory requirements. Organizations should ensure that stakeholders with a role in the organization's use of social media are engaged in the development of a PIA for social media, to include privacy, security, records management, and public affairs officers.

Other Considerations

Organizations must also consider the boundaries between employees' use of social media for authorized official purposes and personal use. While law enforcement officers and public employees have personal constitutional rights to freedom of speech, courts have grappled with distinctions between statements made in an official capacity versus those made as a private citizen. Organizations are encouraged to examine and update their internal policies and procedures to address the personal use of social media sites by officers and/or employees. Organizations should also train officers and employees on the use of social media Web sites and applications to avoid the potential for an employee's personal use of social media to be detrimental to the organization.

Resources

- International Associational of Chiefs of Police (IACP) Center for Social Media: www.iacpsocialmedia.org
- IACP Model Policy for Social Media: www.iacpsocialmedia.org/portals/1/documents/social%20media%20policy.pdf
- OMB Memorandum 10-23, *Guidance for Agency Use of Third-Party Websites and Applications* (June 25, 2010): www.whitehouse.gov/sites/default/files/omb/assets/memoranda_2010/m10-23.pdf
- OMB Memorandum for the Chief Information Officers, Model Privacy Impact Assessment for Agency Use of Third Party Websites and Applications (December 29, 2011): www.whitehouse.gov/sites/default/files/omb/inforeg/info_policy/model-pia-agency-use-third-party-websites-and-applications.pdf

Example of Social Media Privacy Impact Assessments

- DHS Social Networking PIA: www.dhs.gov/xlibrary/assets/privacy/privacy_pia-dhs_socialnetworkinginteractions.pdf
- Program Manager, Information Sharing Environment (PM-ISE) Social Media PIA: www.ise.gov/privacy-impact-assessments

Printed 06/12

Disclaimer:

As a condition to the use of this document and the information contained herein, the Facial Identification Scientific Working Group (FISWG) requests notification by e-mail before or contemporaneously to the introduction of this document, or any portion thereof, as a marked exhibit offered for or moved into evidence in any judicial, administrative, legislative, or adjudicatory hearing or other proceeding (including discovery proceedings) in the United States or any foreign country. Such notification shall include: 1) the formal name of the proceeding, including docket number or similar identifier; 2) the name and location of the body conducting the hearing or proceeding; and 3) the name, mailing address (if available) and contact information of the party offering or moving the document into evidence. Subsequent to the use of this document in a formal proceeding, it is requested that FISWG be notified as to its use and the outcome of the proceeding. Notifications should be sent to: chair@fiswg.org

Redistribution Policy:

FISWG grants permission for redistribution and use of all publicly posted documents created by FISWG, provided that the following conditions are met:

Redistributions of documents, or parts of documents, must retain the FISWG cover page containing the disclaimer.

Neither the name of FISWG, nor the names of its contributors, may be used to endorse or promote products derived from its documents.

Any reference or quote from a FISWG document must include the version number (or creation date) of the document and mention if the document is in a draft status.

Guide for Facial Comparison Training of Reviewers to Competency

1. Scope

1.1 This guide is intended to provide a minimum set of criteria for training of personnel who will conduct facial comparisons at the reviewer level.

1.2 Facial review is a comparison of image-to-image often used in either investigative and operational leads or intelligence gathering applications. Review encompasses a broad range of purposes and levels of rigor involved in the analysis, though it is by nature more rigorous than the assessment process.

1.3 The task of facial review includes, but is not limited to, the use of a facial recognition system to review one-to-many galleries. This task may also include applications involving high volume throughput or escalations from facial assessment.

1.4 The Facial Reviewer role performs a comparison of image(s)-to-image(s) as their primary job function, often used in either investigative and operational leads or intelligence gathering applications.

1.5 Facial Reviewers require a basic level of training to acquire general knowledge and comprehension of the technology and major elements of the facial comparison discipline and use of available tools.

1.6 The intended audience of this document includes agencies and individuals involved in facial comparison at the reviewer level.

2. Terminology

2.1 See ASTM E2916-13 Standard Terminology for Digital and Multimedia Evidence Examination [1]:

3. Summary of Practice

3.1 This guide provides the minimum criteria for training of facial reviewers and should be read in conjunction with the FISWG Guidelines and Recommendations for Facial Comparison Training to Competency and the FISWG Recommendations for a Training Program in Facial Comparison.

3.2 Agencies should include competency testing as a component of training and quality assurance programs as a reliable means of measuring the quality of each trainee's ability to perform work. Competency testing may help identify opportunities for continuing education and training.

3.3 Minimum training requirements for facial reviewers includes demonstrating competency of the following:

[1] For referenced ASTM standards, visit the ASTM website, www.astm.org, or contact ASTM Customer Service at service@asstm.org. For Annual Book of ASTM Standards volume information, refer to the standard's Document Summary page on the ASTM website.

3.3.1 Familiarity with the history of facial comparisons in forensic science to include past and current methods, including the Bertillon method, and their shortcomings.

3.3.2 Understanding of common terminology used in the community.

3.3.3 The user must understand common terminology and should be able to define human face recognition (familiar/eyewitness) and automated facial recognition as well as explain the differences and their distinction from holistic face processing and unfamiliar face matching.

3.3.4 Demonstrate an understanding of the basics of image science including, but not limited to:

3.3.4.1 Vision (e.g., Color, Illumination, Perception)

3.3.4.2 Photography (e.g., Distortions, Pose, Expression, Perspective)

3.3.4.3 Components of digital images and compression

3.3.4.4 Detection of alteration within images (e.g., excessive compression, manipulation)

3.3.4.5 Properties of video (e.g., Limitations, Formats, Extraction of Stills)

3.3.5 Demonstrate proper handling of media, write protection of that media, and generating working copies.

3.3.6 Demonstrate an understanding of the principles of comparison. These principles include:

3.3.6.1 Process of Analysis, Comparison, Evaluation, and Verification (ACE-V)

3.3.6.2 Assessment of facial image quality to determine the value for comparison based on the visibility of facial features

3.3.6.3 The differences between class and individual characteristics, as well as those of transient and stable characteristics.

3.3.6.4 Methods of comparisons

3.3.6.4.1 Morphological Analysis (recommended technique)

3.3.6.4.2 Photo anthropometry (a technique which is not recommended for facial review)

3.3.6.4.3 Superimposition (a technique which is only recommended when used in conjunction with morphological analysis)

3.3.6.5 Conclusion Levels/Scale

3.3.6.6 Validation of Facial Comparisons (i.e., Ability to render proper conclusions)

3.3.6.7 Overview and effects of cognitive bias, to include confirmation bias

3.3.6.8 Understanding the necessity for verification by a second trained reviewer

3.3.7 Knowledge of automated facial recognition systems, to include, but not limited to:

3.3.7.1 User input and operation

3.3.7.2 System operation and output

3.3.7.3 Facial recognition algorithm limitations including, but not limited to:

3.3.7.3.1 Imaging conditions (e.g., image quality, pose)

3.3.7.3.2 Accessories (e.g., eyeglasses, jewelry)

3.3.7.3.3 Obstructions (e.g., masks, scarves, head coverings)

3.3.8 Familiarity with basic image processing operations (e.g., brightness and contrast adjustments, rotations, cropping)

3.3.9 Familiarity with the bones that comprise the skull and the overlaying musculature.

3.3.10 Knowledge of the ASTM E3149-18 Standard Guide for Facial Image Comparison Feature List for Morphological Analysis, to include, but not limited to:

3.3.10.1 Hair (e.g., hairline, baldness)

3.3.10.2 Eyes and Eyebrows

3.3.10.3 Nose

3.3.10.4 Mouth

3.3.10.5 Ears

3.3.10.6 Facial lines, marks, and scars

3.3.11 Knowledge of the variable nature of the human face over time, the level of permanence of individual features, and understand the results of aging.

3.3.12 Knowledge of alterations of the face, both temporary and permanent.

3.3.12.1 Examples of temporary changes are: cosmetics, weight changes, hair color changes, wounds, and abrasions.

3.3.12.2 Examples of permanent changes are: scars, surgical alterations, tattoos, and piercings.

3.4 Minimum training requirements for facial reviewers includes demonstrating awareness of the following:

3.4.1 Court testimony.

3.4.1.1 Knowledge of individual agency policies and procedures is beyond the scope of this document and is the responsibility of the user's agency.

3.4.2 Their agency's authorities and policies regarding acceptable use and dissemination;

3.4.3 Relevant judicial decisions that govern admittance of scientific evidence in court (e.g. Daubert).

3.4.4 The perception of facial recognition in the legal community.

3.4.5 Proper chain of custody, documentation and notes, reporting of results, and technical review.

3.4.6 Common misconceptions created by popular media to include fictional television shows, novels, and movies, cumulatively known as "The CSI Effect."

4. Keywords

4.1 Facial Reviewer, Training, Facial Identification, Facial Comparison

FISWG documents can be found at: www.fiswg.org

Disclaimer:

As a condition to the use of this document and the information contained herein, the Facial Identification Scientific Working Group (FISWG) requests notification by e-mail before or contemporaneously to the introduction of this document, or any portion thereof, as a marked exhibit offered for or moved into evidence in any judicial, administrative, legislative, or adjudicatory hearing or other proceeding (including discovery proceedings) in the United States or any foreign country. Such notification shall include: 1) the formal name of the proceeding, including docket number or similar identifier; 2) the name and location of the body conducting the hearing or proceeding; and 3) the name, mailing address (if available) and contact information of the party offering or moving the document into evidence. Subsequent to the use of this document in a formal proceeding, it is requested that FISWG be notified as to its use and the outcome of the proceeding. Notifications should be sent to: chair@fiswg.org

Redistribution Policy:

FISWG grants permission for redistribution and use of all publicly posted documents created by FISWG, provided that the following conditions are met:

Redistributions of documents, or parts of documents, must retain the FISWG cover page containing the disclaimer.

Neither the name of FISWG, nor the names of its contributors, may be used to endorse or promote products derived from its documents.

Any reference or quote from a FISWG document must include the version number (or creation date) of the document and mention if the document is in a draft status.

Minimum Training Criteria for Assessors Using Facial Recognition Systems

1. Purpose

1.1. This document is intended to provide a minimum set of criteria for training of personnel who conduct facial assessment in a quick throughput environment using a facial recognition (FR) system to assist them with meeting their objective.

2. Introduction

2.1. The task of facial assessment is a quick comparison of facial image-to-image or image-to-person. The task of facial assessment includes, but it not limited to a quick comparison of image-to-image or image-to-person typically carried out in screening and access control applications or field operations. Due to time constraints, assessment is the least rigorous of all facial comparison categories.

2.2. Automated facial recognition systems that provide a one-to-many search candidate list require a user to review and process the results. Assessors using an FR system should not use results from the system alone, however, results should be used in conjunction with additional resources.

2.3. Facial Assessors are not specialists in facial comparison, but the role requires an awareness of the major elements and limitations of the facial comparison discipline and training in the use of available tools.

2.4. The intended audience of this document includes agencies and individuals involved in facial comparison at the assessment level using FR systems.

3. Agency Considerations Related to Training

3.1. Agencies must document completion of training and the competency of their users.

3.2. Agencies must include competency testing as a component of training and quality assurance programs as a reliable means of measuring the quality of each user's ability to perform work. Competency testing measures individual performance and may help identify opportunities for continuing education and training.

3.3. The material provided below represents the minimum training criteria which may be tailored to meet the individual agency's operational needs. FISWG discourages the use of a facial recognition system by users who have not successfully completed the minimum training and strongly encourages further user training beyond the minimum criteria. and. Resources for additional training information include, but are not limited to, *FISWG Guidelines for Recommendations for Facial Comparison Training to Competency* and *FISWG Recommendations for a Training Program in Facial Comparison*.

4. Training Requirements

4.1. The user should be familiar with the history of facial comparisons in forensic science to include past methods, such as the Bertillon method, and their shortcomings.

4.2. The user must understand common terminology and should be able to define human face recognition (familiar/eyewitness) and automated facial recognition, as well as explain the differences and their distinction from holistic face processing and unfamiliar face matching.

4.3. The user must demonstrate an understanding of the basics of image science including, but not limited to:

- 4.3.1. Vision (e.g., Color, Illumination, Perception)
- 4.3.2. Photography (e.g., Distortions, Pose, Expression, Perspective)
- 4.3.3. Components of digital images and compression (e.g., knowledge of sensors, pixels, resolution)Possible alteration of images (e.g., excessive compression, manipulation)
- 4.3.4. Properties of video (e.g., Limitations, Formats, Extraction of Stills)

4.4. The user should be familiar with the proper handling of media, write protection of that media, and generating working copies.

4.5. The user must understand the principles of comparison. These principles include:

- 4.5.1. Process of Analysis, Comparison, Evaluation and Verification (ACE-V)
- 4.5.2. Assessment of facial image quality to determine the value for comparison based on visibility of facial features.
- 4.5.3. The differences between class and individual characteristics, as well as those of transient and stable characteristics.
- 4.5.4. Methods of facial comparisons
  - 4.5.4.1. Morphological Analysis (the FISWG-recommended technique)

4.5.4.2. Superimposition (a technique which is only recommended by FISWG when used in conjunction with morphological analysis)

4.5.4.3. Photo-anthropometry (a technique which is not recommended by FISWG for facial review)

4.5.5. Conclusion Levels/Scale

4.5.6. Validation of Facial Comparison (i.e., Ability to render proper conclusions)

4.5.7. Overview and effects of cognitive bias, to include confirmation bias

4.5.8. Understanding of the necessity for verification by a second trained reviewer

4.6. The user should have a general knowledge of automated facial recognition systems, to include, but not limited to:

4.6.1. User input and operation

4.6.2. System operation and output

4.6.3. Facial recognition algorithm limitations including, but not limited to:

4.6.3.1. Imaging conditions (e.g., image quality, lighting, pose)

4.6.3.2. Obstructions and Accessories (e.g., eyeglasses, jewelry, masks, scarves, head coverings)

4.7. The user should be familiar with basic image processing operations (e.g., brightness and contrast adjustments, rotations, cropping)

4.8. The user should be familiar with the bones that comprise the skull and the overlying musculature.

4.9. The user must have a basic knowledge of the FISWG Facial Image Comparison Feature List for Morphological Analysis (see also, ASTM E3149-18 Standard Guide for Facial Image Comparison Feature List for Morphological Analysis), to include, but not limited to:

- 4.9.1. Hair (e.g., hairline, baldness)
- 4.9.2. Eyes and Eyebrows
- 4.9.3. Nose
- 4.9.4. Mouth
- 4.9.5. Ears
- 4.9.6. Facial lines, marks and scars

4.10. The user should be aware of the variable nature of the human face over time, the level of permanence of individual features, and understand the results of aging.

4.11. The user should be aware of alterations of the face, both temporary and permanent.

- 4.11.1. Examples of temporary changes are: cosmetics, weight changes, hair color changes, wounds, and abrasions.
- 4.11.2. Examples of permanent changes are: scars, surgical alterations, tattoos, and piercings.

4.12. Users of facial recognition systems should be prepared to testify, regardless of their specific job duties. Basic training for court testimony, including knowledge of individual agency policies and procedures is beyond the scope of this

document and is the responsibility of the user's agency. However, users of facial recognition systems should be aware of the following:

4.12.1. Their agency's authorities and policies regarding acceptable use and dissemination.

4.12.2. Relevant judicial decisions that govern admittance of scientific evidence in court (e.g. Daubert).

4.12.3. The perception of facial recognition in the legal community.

4.12.4. Proper chain of custody, documentation and notes, reporting of results, and technical review.

4.12.5. The possibility of digital manipulation or alteration of the image(s).

4.12.6. Common misconceptions created by popular media to include fictional television shows, novels, and movies, cumulatively known as 'The CSI Effect'.

FISWG documents can be found at: www.fiswg.org

Disclaimer:

As a condition to the use of this document and the information contained herein, the Facial Identification Scientific Working Group (FISWG) requests notification by e-mail before or contemporaneously to the introduction of this document, or any portion thereof, as a marked exhibit offered for or moved into evidence in any judicial, administrative, legislative, or adjudicatory hearing or other proceeding (including discovery proceedings) in the United States or any foreign country. Such notification shall include: 1) the formal name of the proceeding, including docket number or similar identifier; 2) the name and location of the body conducting the hearing or proceeding; and 3) the name, mailing address (if available) and contact information of the party offering or moving the document into evidence. Subsequent to the use of this document in a formal proceeding, it is requested that FISWG be notified as to its use and the outcome of the proceeding. Notifications should be sent to: chair@fiswg.org

Redistribution Policy:

FISWG grants permission for redistribution and use of all publicly posted documents created by FISWG, provided that the following conditions are met:

Redistributions of documents, or parts of documents, must retain the FISWG cover page containing the disclaimer.

Neither the name of FISWG, nor the names of its contributors, may be used to endorse or promote products derived from its documents.

Any reference or quote from a FISWG document must include the version number (or creation date) of the document and mention if the document is in a draft status.

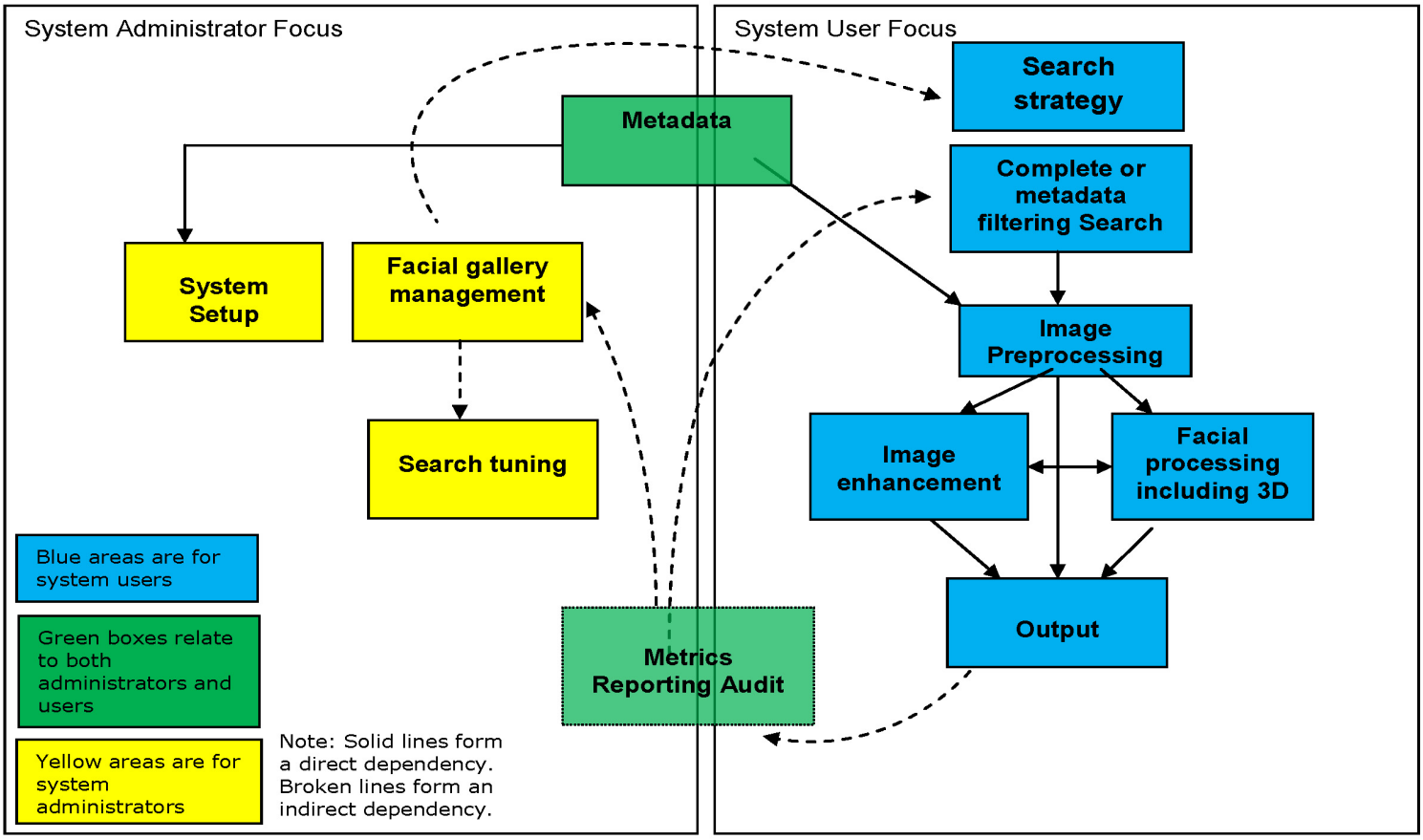
Section 4.2 Methods and Techniques

Facial Recognition System: Methods and Techniques

This document provides a general outline of **Methods and Techniques** that can be helpful or considered when planning or operating a Facial Recognition (FR) system. The goal of this document is to provide guidance on methods and techniques to increase the likelihood of obtaining a true match in the candidate list for a submitted probe within a 1:N search. Please refer to the FISWG web site for guidance on human 1:1 comparison processes that may be required following a 1:N search.

Figure 1 is important to both system administrators and system users as it displays the relationship and information represented by the system, the flow of search strategies, and the management of the data in the facial gallery.

Figure 1 – System Flow (post enrollment)



NOTE: FISWG defines metadata binning as: A technique used by a FR system to organize enrollment of data to facilitate and optimize searching using filters based on information associated with an image.1

Target audiences:

- System administrators or developers of the FR system.
  - System developers are responsible for the overall design of the system features that allow and enable these methods and techniques.
  - System administrators are responsible for verification and proper deployment, implementation, and usage of these methods and techniques.
- System users.
  - System users are the examiners, operators, or other personnel who actually utilize the system for facial searching purposes.

A number of areas are described in overview below. Each area will be covered in depth in future FISWG standalone specific documents:

1. Metadata system setup and usage
2. Facial gallery management
3. Enrollment of the facial image
4. Search tuning
5. Search strategy and options
6. Image preprocessing
7. Eye locations
8. Metrics reporting auditing

1. Metadata system setup and usage

   Metadata is anything associated with but excluding the facial image and can include a system generated identity number for the person and/or gender, image header information, age, race, scars, marks, tattoos, ethnicity, etc.

   Metadata usage can be broken down into two main areas: system setup of the metadata by the system administrators and actual usage of the metadata by the system users.

   Metadata binning and subsequent filtering is an efficient approach that utilizes investigative data to refine a search and improve search results. If the metadata associated with the probe image is available to the practitioner and the FR system being used allows a metadata search, metadata filtering could be used to refine the initial search or to further refine the search results. Agency policy should govern at what point metadata is used in the search process, and user preference or agency policy will determine whether filters are added separately or jointly. If refining a search using metadata filters is an option, experimenting to determine the results each filter will produce will assist the practitioner in learning the limits of this type of search.

   It is suggested that the initial search be conducted using only the probe facial image, with no metadata search included. This will result in the largest-possible candidate list for comparison purposes. Subsequent searches using metadata as a filtering tool can then be performed in an effort to produce a more specific result and the best candidate list for analysis. It is prudent to use metadata searches even if a likely candidate is returned as a

[1] *FISWG Glossary Version 1.1, dated 2/12/2012*

result of the initial search, as there may be additional photos/candidates available for comparison within the database that a metadata search would disclose. It is important to note that a photo-only or metadata-only search may result in candidates that the other method of searching would not. If the option is available, a subsequent metadata-only search may produce an additional useful candidate list.

Using metadata filtering to refine a search can also be used to test a FR system algorithm. Limiting a search to specific parameters while searching for an image that is known to be a part of the FR database can disclose algorithm problems if the known photo is not a part of the resulting gallery. Additionally, by observing how a system responds, for example, to an image-only search vs. a metadata-only search, a practitioner can improve his/her own search strategy.

Metadata system setup is the phase where the metadata accessible for FR system usage is defined and categorized. This requires the textual information (e.g., demographic, biographic, contextual etc.) associated with the facial images to be defined as pick lists, numeric ranges, dates, or free text.

Metadata may also be created from indirect information not directly associated with a person. Examples here include:

a) Recidivism
b) Criminal behavior correlations
c) Gang or other affiliations
d) Watchlisting
e) Categorizing metadata sets into larger groupings (e.g., Regional Originating Agency (ORI) sets)

If metadata is known at the time of the FR enrollment then this information can be used (e.g. binning) to logically reduce the size of the gallery to be searched/filtered in a controlled and deterministic manner. Usage of metadata should be appropriately integrated into the overall search strategy because improper usage can be detrimental to providing successful search results. If the consistency of the metadata is low (i.e. there are data entry errors where, for example, gender is incorrectly entered) then filtering based on this demographic will result in higher error rates and the correct match to the probe could be filtered out.

If binning is utilized then it should be understood that metadata usage is a logical pre-filter and is separate from the algorithmic portion of the biometric matching process. If the consistency is known to be high, binning can improve performance, both in time and likelihood of returning a true mate.

2. Facial gallery management

Facial gallery management can be described as:

a) Monitoring and maintenance processes done on the overall gallery as it grows and changes.
b) Facial search techniques tuned to the galleries that are not static, can be changed or adjusted.
c) Applying user access controls and restrictions to subsets of data that have been deemed operationally sensitive.

Operational performance can be more effective if data is organized per algorithm sensitive characteristics and appropriate search strategies are used. For example, small images may require a different search strategy than large images. Further, off pose face images may be better suited for one algorithm while frontal images may produce better results using

another algorithm. Data quality metrics, demographics, and contextual data can all be used to analyze, profile, locate, present, repair, or exclude images.

Facial gallery management can be broken down into two main areas: data profiling and data cleansing.

Data Profile

a) Facial galleries can be collections of various types and quality of imagery from different capture systems that can be characterized based on their core similarities (e.g., image file size, image quality, expression, etc.). This has also been referred to as "sameness". Galleries should be profiled in order to gain an understanding as to how many collections exist.
b) These collections can be managed and search strategies defined taking into consideration the aforementioned characteristics of the galleries that may improve search performance.
c) Proper profiling involves knowing the collections in the facial galleries. Operational pilots have shown significant increases in accuracy by choosing the appropriate search strategy for a given image set within a larger gallery of assorted images.

Data Cleansing

a) Many images in a facial gallery are sub-optimal due to reasons that include but are not limited to:
    - Non-frontal faces
    - Images not of a person
    - Incorrectly detected eye positions
b) These images need to be identified so they may be isolated, corrected, or marked for exclusion

3. Enrollment of the facial image

The timing of the enrollment of a facial image into an automated FR system will have an effect on 1) whether subsequent images are providing the most-comprehensive search and 2) the timing of a response to a requestor. The best-case scenario would consist of a near real-time operational environment – an FR system enrolling an image as the image is entered into the system to be searched. This would ensure that the image is enrolled to the system's photo gallery immediately, that it is immediately available to be searched against subsequent probe images, and that it is searched against every previously-submitted image maintained within the database. However, since all FR systems are not the same, this is not always the case.

With a time-delayed environment, some amount of time will pass before a probe photo is enrolled into the database following a search. If subsequent probes are searched prior to previous probes being enrolled (i.e., if an agency waits until a certain time of day to enroll all of the day's probe images), a possible candidate(s) may not yet be in the system's database and, therefore, cannot/will not be included in the resulting candidate list. Conversely, if an agency waits to search probes until the system has been updated by the enrollment of the day's previously-searched probes, searches will not be performed in a timely manner and investigations may be impeded. This is also true of batch process enrollments.

Practitioners should be aware of their agency's system enrollment policy and adjust their search strategy accordingly. If the system environment is not real-time the search of a probe image prior to the day's system update may necessitate a re-search of the probe once all of the day's images have been enrolled.

4. Search tuning
   The purpose of search tuning is to improve overall system performance. Search tuning is defined as analysis or testing that has been undertaken on operational data that results in a set of predefined or range(s) of settings or options that can be used when searching. Any search tuning should incorporate information from (i) system developer and/or integrator, (ii) objective testing/testers and (iii) operational user analysis with respect to the given FR system, its data, and its targeted goals.

   Information from the system integrator should include but is not limited to:
   a) What is the overall approach used for the FR system? Describe the FR system sensitivity to: geometric shapes of the face, facial features, skin texture, facial landmarks, or other facial representations.
   b) How much roll, pitch, or yaw can be tolerated before pose correction should be considered?
   c) Is there any known bias in the system (e.g., age, ethnic, other)?
   d) Is multi-pass searching used? If so what options exist to vary the search pass settings?
   e) Is there a trade-off between accuracy and search speed? If so, how is the intensity of the searching changed? Who can make these changes?
   f) How does facial gallery growth and size impact FR search times?
   g) How do you interpret a facial match score?
   h) Is any scoring normalization used or available? If so what types and kinds? Is each gallery dependent or gallery independent?
   i) Are there any effects on facial match scores as the gallery size changes e.g. quality of match performance with more images of more candidates?

   Objective tests can then help provide assurance that any information provided is accurate when it applies to critical statements or assumptions. Objective tests should be performed on ground truth data. If it is not possible to ground truth operational data then the test data should aim to be as representative as possible to the intended data type(s) of the system. For example, if the system is to be used with a combination of mugshot and surveillance images, then testing should be undertaken on galleries consisting of both of these image types.

5. Search Strategy
   As noted in previous FISWG documents, "it must be recognized that agencies (and individuals) perform facial comparison for a wide variety of purposes, often under operational conditions that do not allow for a great deal of time or effort to be expended. Agencies that choose to utilize such methods must recognize this fact and the associated risks (i.e., greater chance of error)."2 This applies to other operational constraints including, but not limited to, enrollment of images, varying system algorithms, requestor's directives, and agency policies. A comprehensive search is a trade-off. If agency-specific constraints such as workload, workforce, and/or deadlines and outside influences such as a requestor's directives are predominant concerns, results will suffer. Search strategies employed by practitioners should take into consideration any known policies, constraints, and customer expectations.

[2] *FISWG Guidelines for Facial Comparison Methods Version 1.0, dated 2/2/2012*

Agency policy and outside influence will dictate the extent of searches performed. Any system designed to hold operationally sensitive data needs to consider levels of user access and restrictions to subsets of data. Operational policy should be an agency decision, but workload, workforce, and deadline may dictate and constrain searching strategy/possibilities and, therefore, results. As previously noted by FISWG, "Facial comparisons are performed for a number of reasons and the comparison methods employed should be chosen based on the timeframe required for a decision and the level of confidence required. Comparisons that need to be immediate require the use of faster processes that will necessarily lead to a result with a lower confidence. In certain scenarios, this lower confidence is an acceptable trade-off for the speed of the analysis."3 This applies to a modified searching strategy resulting from policy-driven or requestor constraints, as well.

Requesting agencies potentially constrained by policy, may ask that certain procedures be followed, such as a request to search by specific metadata, to search additional databases that are external to the initial searching agency, or even to request there be a certain (i.e., limited) number of images in the candidate list that is returned. In such cases, search results will be dependent on information provided by the contributing agency, and results may differ from those that would be produced had no constraints or directives been issued.

In all contingencies, the practitioner must understand his/her FR system's capabilities and limitations before asking it to search by specific information, and in order to develop the best strategy for his/her operational environment and the constraints put in place by the agency and/or the requestor.

Search options are defined as the options or feature sets a user has at their disposal when doing a facial search. This is the culmination of all methods and techniques defined within this document, that if done properly should increase the likelihood of a successful search.

Accurate comparison of facial images is highly-dependent on the quality of both the probe and the gallery image. A practitioner's ability to note similarities and differences between the probe and gallery image(s) is reduced when both are not of optimal image quality, and he/she may be unable to reach a definitive conclusion.

Comparison of:

- **A high-quality probe against the high-quality portions of the facial gallery**

  As FISWG has noted previously, "Optimal images for facial comparison are high resolution and have sufficient focus to resolve features of interest, such as blemishes and wrinkles, with minimal compression artifacts or distortion…"4 The obvious advantage to comparing a high-quality probe against a high-quality gallery image is that, with pristine images, the practitioner will be able to clearly view, on each image, every feature that is typically compared during the morphological analysis of the face. The higher the quality of the probe image, the better the chance of producing a candidate list that will result in a likely candidate and the stronger the conclusion that can be drawn.

---

[3] *FISWG Guidelines for Facial Comparison Methods Version 1.0, dated 2/2/2012*
[4] *FISWG Guidelines for Facial Comparison Methods Version 1.0, dated 2/2/2012*

- **A low-quality probe against the high-quality portions of the facial gallery**

  Each agency and practitioner will have his/her own definition of what constitutes a low-quality probe image. These include, but are not limited to, distorted photos, low resolution face, and limited dynamic range, each of which impede the practitioner's ability to clearly discern the subject's facial features. A FR system may accept a less-than-optimal probe image, but the lack of discernible facial features will result in a less-than-optimal candidate list, regardless of quality of the photos within the FR system. If an experienced practitioner with the proper training in the analysis of such photos is able to discern a clear feature on a poor-quality probe image, he/she will be more likely to match the probe to a gallery image; however, the conclusion drawn may be weak. Metadata binning may be considered as a way to improve searching/filtering candidates that closely match general, obvious, or known features of the probe image. The best-case scenario may be to utilize this situation as an opportunity to eliminate those photos with obvious differences, and/or offer any conclusions drawn to the requestor as an investigative lead as opposed to identification.

- **A high-quality probe against the low quality portions of the facial gallery**

  While a high-quality probe will increase the probability of a more thorough image search against the photos within a FR system and may produce a more comprehensive candidate list for comparison, the gallery may still include images of low quality. As with the scenario noted above, if an experienced practitioner with the proper training in the analysis of such photos is able to discern a clear feature on a poor-quality probe image, he/she will be more likely to match the probe to a gallery image; however, the conclusion drawn may be weak. Metadata binning may be considered as a way to improve searching/filtering candidates that closely match general, obvious, or known features of the probe image. The best-case scenario may be to utilize this situation as an opportunity to eliminate those photos with obvious differences, and/or offer any conclusions drawn to the requestor as an investigative lead as opposed to identification.

- **A low-quality probe against the low-quality portions of the facial gallery**

  Obviously the most-challenging scenario, the submission of a low-quality probe image for search by an FR system will return a less-than-optimal candidate list, and the comparison of a low-quality probe against a low-quality gallery image should be attempted only by an experienced practitioner who has been properly trained in handling this type of comparison. Metadata filtering may produce a more productive candidate list than image search alone, but poor quality renders it difficult to discern blemishes, shapes, and features of the face. Practitioners will be less able to render definitive conclusions. Eliminations may be easier to make based on gender, race, and ethnicity.

Example operational scenarios that should be discussed include:

a) When and how to use metadata filtering when searching
   - Are there specific instances where metadata filtering can be used or should not be used?
   - When searching the gallery, should the search start with no filtering, followed by adding metadata filters? Or should metadata filtering be applied on the initial searches and then removed or altered based on the character and content of the result sets?
b) How is the searching strategy affected by having multiple probes?
   - Using the same image with different variations from image preprocessing
   - Using multiple images of the same person of interest in entirely different images
c) How or when can the number of results be changed to augment the search process?
d) How can the options or features in the biometric algorithm be used to augment the search process?

Search strategies should also be planned around any known operational constraints. An example of this is how or when new images are enrolled into the gallery and does this affect how facial searching is done on new probes that need to be searched? If gallery images are enrolled twice a day, does this cause a deliberate time delay in searching a new facial image?

Within the context of this document, metadata filtering is assumed to be done within the search process and not a post search user based operation. If the client used for reviewing search results offers post search filtering, then this can greatly enhance the reviewing of candidate list results.

6. Image preprocessing

Ideally, image preprocessing enhances a probe facial image in order to improve the matching prospects. The system developer should provide any appropriate guidelines for optimized facial data to be used by the system. Preprocessing should only be done on poor quality images as determined by the quality attributes provided by the developer or quality metrics supplied by the face recognition system. Improper use of image preprocessing can degrade system performance and therefore only properly trained personnel using industry accepted image processing applications within approved agency guidelines should perform image preprocessing.

Image preprocessing can include both image enhancement and facial processing. In all steps the original image is always preserved for reference and forensic comparison purposes. It is left up to agency policy to determine if the original image should always be searched.

a) Image enhancement uses standardized 2D filters including but not limited to image lighting, histogram equalization, color corrections, de-blur, etc.) Such enhancements are strictly reliant on information within the image itself. The geometric aspects of the person in the facial image are NOT changed when doing this.
b) Facial preprocessing is applied to just the face to clarify and improve the facial image in order to render a more compliant search probe. Techniques include three dimensional modeling such as pose correction. These are separate and distinct from two dimensional modifications because the geometric aspects of the person in the facial image are changed when doing this.

Some current FR systems provide options, although they may be limited, that will allow a

practitioner to enhance a probe image, as necessary, once it has been submitted to the system for search. Much like enhancements made with software such as Photoshop®, these options will permit a practitioner to make changes to the original probe photo, therefore allowing a more comprehensive search and possibly resulting in higher ranked or additional candidate list images. If a FR system produces a poor candidate list, the user can take advantage of image preprocessing.

Such enhancements could include, but are not limited to:

a) Adjusting brightness
b) Adjusting colors/tinting
c) Adjusting contrast
d) Cropping the image
e) Enlarging the image
f) Adjusting roll, pitch, or yaw
g) Marking the center of eye
    - May help algorithm with eye placement
    - Distance between eyes may also assist search parameters
h) Adding metadata to the search (e.g., sex, race, etc.) after the initial image search

A practitioner may find that searching a number of probe photos, the same image with different variations of enhancements, and/or multiple images of the same subject – provided the images are clear – improves the chances of an image search resulting in a candidate. However, regardless of how many probes are submitted by a requestor or to what extent the practitioner enhances the probe, all available probe images should be searched, and the same basic search strategies should be used.

Using Photoshop® or comparable software, probe images can be modified from color to black and white or enhanced, as necessary, to reveal facial features. At the discretion of the practitioner, the image search can begin with the best probe image or all available probes can be submitted for search at one time. Regardless of the search order, all available probes should be searched, whether it is assumed that any will be rejected by the system, or whether a candidate list has already been produced as a result of any other probe. Using this approach will ensure a comprehensive search and a more robust candidate list for comparison purposes. All candidate lists resulting from the search of any of the probe images should be reviewed.

If metadata is submitted with a probe image, a metadata search should be conducted, regardless of the size of the candidate list returned as a result of the image searched.

7. Eye Locations

In all steps involving image preprocessing, it is key to ensure that proper eye location and verification is done. This is either a manual placement of eye locations on an image or the verification that the FR algorithm can automatically locate eyes in the final search probe.

Eye location verification is a key part of the facial image search process, and essential to an accurate image search by an automated FR system, as it improves the algorithm search. Agencies should take this into consideration when purchasing an automated FR system. Taking into consideration all existing FR systems, however, a practitioner may not have the option of marking the center of the probe photo's eyes prior to search. To ensure searching consistency, each agency should know how their FR system operates. For example will it mark the eyes (or the chin, or the ears)? Individual agencies should establish an eye location verification policy that will ensure that the center of the eye is marked prior to searching or, if this feature is not available, that the probe photo's roll, pitch, and/or yaw is

adjusted so the eyes are level. Agencies must be aware of how their FR system operates – this will drive policy.

8. Metrics Reporting and Auditing
   This is defined as the collection, summary, and analysis of any and all information presented to, acted on, or produced by the FR system. The outcome of this can be used to understand the system operation, defend the performance of the system, or develop understandings of how to improve or optimize the system as a whole.

   The following FR performance metrics may include:

   a) Searches done
      - Date and time
      - Workstation
      - User
      - Search strategy
      - Metadata filter(s) applied
      - Probe characteristics
      - Search results
   b) Average search time
      - Search strategy
      - Facial gallery size
      - Metadata filter(s) applied
   c) Failure to acquire / inability to create template
   d) Characteristics of the result sets
      - Number of results
      - Scores and distributions
      - Metadata of interest
   e) Confirmed matches
      - Scoring
      - Ranking
   f) Overall quality of the facial images as it pertains to the FR matching

   These metrics should be routinely reviewed for continual operational tuning and overall effectiveness.

========== END of document ==========

Reference List

FISWG documents can be found at: www.FISWG.org

Section	Title
Section 1	Glossary of Terms
Section 2	Facial Comparison Overview
Section 3	Guidelines and Recommendations for Facial Comparison Training to Competency
Section 4	Guidelines for Specifications, Procurement, Deployment, and Operations of Facial Recognition Systems
Section 5	Capture and Equipment Assessment for Facial Recognition Systems
Section 6	Guidelines for Facial Comparison Methods
Section 7	Recommendations for a Training Program in Facial Comparison
Section 8	
Section 9	
Section 10	

Face recognition accuracy of forensic examiners, superrecognizers, and face recognition algorithms

P. Jonathon Phillips[a,1], Amy N. Yates[a], Ying Hu[b], Carina A. Hahn[b], Eilidh Noyes[b], Kelsey Jackson[b], Jacqueline G. Cavazos[b], Géraldine Jeckeln[b], Rajeev Ranjan[c], Swami Sankaranarayanan[c], Jun-Cheng Chen[d], Carlos D. Castillo[d], Rama Chellappa[c], David White[e], and Alice J. O'Toole[b]

[a]Information Access Division, National Institute of Standards and Technology, Gaithersburg, MD 20899; [b]School of Behavioral and Brain Sciences, The University of Texas at Dallas, Richardson, TX 75080; [c]Department of Electrical and Computer Engineering, University of Maryland Institute for Advanced Computer Studies, University of Maryland, College Park, MD 20854; [d]University of Maryland Institute for Advanced Computer Studies, University of Maryland, College Park, MD 20854; and [e]School of Psychology, The University of New South Wales, Sydney, NSW 2052, Australia

Edited by Thomas D. Albright, The Salk Institute for Biological Studies, La Jolla, CA, and approved April 30, 2018 (received for review December 13, 2017)

Achieving the upper limits of face identification accuracy in forensic applications can minimize errors that have profound social and personal consequences. Although forensic examiners identify faces in these applications, systematic tests of their accuracy are rare. How can we achieve the most accurate face identification: using people and/or machines working alone or in collaboration? In a comprehensive comparison of face identification by humans and computers, we found that forensic facial examiners, facial reviewers, and superrecognizers were more accurate than fingerprint examiners and students on a challenging face identification test. Individual performance on the test varied widely. On the same test, four deep convolutional neural networks (DCNNs), developed between 2015 and 2017, identified faces within the range of human accuracy. Accuracy of the algorithms increased steadily over time, with the most recent DCNN scoring above the median of the forensic facial examiners. Using crowd-sourcing methods, we fused the judgments of multiple forensic facial examiners by averaging their rating-based identity judgments. Accuracy was substantially better for fused judgments than for individuals working alone. Fusion also served to stabilize performance, boosting the scores of lower-performing individuals and decreasing variability. Single forensic facial examiners fused with the best algorithm were more accurate than the combination of two examiners. Therefore, collaboration among humans and between humans and machines offers tangible benefits to face identification accuracy in important applications. These results offer an evidence-based roadmap for achieving the most accurate face identification possible.

face identification | forensic science | face recognition algorithm | wisdom-of-crowds | machine learning technology

Societies rely on the expertise and training of professional forensic facial examiners, because decisions by professionals are thought to assure the highest possible level of face identification accuracy. If accuracy is the goal, however, the scientific literature in psychology and computer vision points to three additional approaches that merit consideration. First, untrained "superrecognizers" from the general public perform surprisingly well on laboratory-based face recognition studies (1). Second, wisdom-of-crowds effects for face recognition, implemented by averaging individuals' judgments, can boost performance substantially over the performance of a person working alone (2–5). Third, computer-based face recognition algorithms over the last decade have steadily closed the gap between human and machine performance on increasingly challenging face recognition tasks (6, 7).

Beginning with forensic facial examiners, remarkably little is known about their face identification accuracy relative to people without training, and nothing is known about their accuracy relative to computer-based face recognition systems. Independent and objective scientific research on the accuracy of forensic facial practitioners began in response to the National Research Council report *Strengthening Forensic Science in the United States: A Path Forward* (8; cf. ref. 9). In the most comprehensive study to date (3), forensic facial examiners were superior to motivated control participants and to students on six tests of face identity matching. However, image pairs in these tests appeared for a maximum of 30 s. Identification decisions in a forensic laboratory typically require days or weeks to complete and are made with the assistance of image measurement and manipulation tools (10). Accordingly, the performance of forensic facial examiners in ref. 3 represents a lower-bound estimate of the accuracy of examiners in practice.

Superrecognizers are untrained people with strong skills in face recognition. Multiple laboratory-based face recognition tests of these individuals indicate that highly accurate face identification can be achieved by people with no professional training (1). Superrecognizers contribute to face recognition decisions made in law enforcement (11, 12) but have not been compared with forensic examiners or machines.

The term wisdom-of-crowds refers to accuracy improvements achieved by combining the judgments of multiple individuals to make a decision. Face recognition accuracy by humans can be boosted substantially by crowd-sourcing responses (2–5),

Significance

This study measures face identification accuracy for an international group of professional forensic facial examiners working under circumstances that apply in real world casework. Examiners and other human face "specialists," including forensically trained facial reviewers and untrained superrecognizers, were more accurate than the control groups on a challenging test of face identification. Therefore, specialists are the best available human solution to the problem of face identification. We present data comparing state-of-the-art face recognition technology with the best human face identifiers. The best machine performed in the range of the best humans: professional facial examiners. However, optimal face identification was achieved only when humans and machines worked in collaboration.

Author contributions: P.J.P., A.N.Y., D.W., and A.J.O. designed research; R.R., S.S., J.-C.C., C.D.C., and R.C. contributed new reagents/analytic tools; P.J.P., A.N.Y., Y.H., C.A.H., E.N., K.J., J.G.C., G.J., and A.J.O. analyzed data; R.R., S.S., J.-C.C., C.D.C., and R.C. implemented and ran the face recognition algorithms; and P.J.P. and A.J.O. wrote the paper.

Conflict of interest statement: The University of Maryland is filing a US patent application that will cover portions of algorithms A2017a and A2017b. R.R., C.D.C., and R.C. are coinventors on this patent.

This article is a PNAS Direct Submission.

[1]To whom correspondence should be addressed. Email: jonathon@nist.gov.

This article contains supporting information online at www.pnas.org/lookup/suppl/doi:10.1073/pnas.1721355115/-/DCSupplemental.

Published online May 29, 2018.

PSYCHOLOGICAL AND COGNITIVE SCIENCES

including for forensic examiners in a time-restricted laboratory experiment (3). Combining human and machine face identification judgments also improves accuracy over either one operating alone (5). The effect of fusing the judgments of professionals and algorithms has not been explored.

Computer-based face recognition systems now assist forensic face examiners by searching databases of images to generate potential identity matches for human review (13). Direct comparisons between human and machine accuracy have been based on algorithms developed before 2013. At that time, algorithms performed well with high-quality frontal images of faces with minimal changes in illumination and expression. Since then, deep learning and deep convolutional neural networks (DCNNs) have become the state of the art for face recognition (14–18). DCNNs can recognize faces from highly variable, low-quality images. These algorithms are often trained with millions of face images of thousands of people.

Our goal was to achieve the most accurate face identification using people and/or machines working alone or in collaboration. The task was to determine whether pairs of face images showed the same person or different people. Image pairs were prescreened to be highly challenging based on data from humans and computer algorithms. Images were taken with limited control of illumination, expression, and appearance. Fig. 1 shows two example pairs (all pairs are shown in *SI Appendix*, Figs. S8–S14). To provide a comprehensive assessment of human accuracy, we tested three face specialist groups (forensic facial examiners, forensic facial reviewers, and superrecognizers) and two control groups (fingerprint examiners and undergraduate students). Humans responded on a 7-point scale that varied from high confidence that the pair showed the same person (+3) to high confidence that the pair showed different people (−3). We also tested four face recognition algorithms based on DCNNs developed between 2015 and 2017. Algorithm responses were real-valued similarity scores indicating the likelihood that the images showed the same person. The five subject groups and four algorithms were tested on the same image pairs. Facial examiners, reviewers, superrecognizers, and fingerprint examiners had 3 mo to complete the test. Students took the test in a single session.

Forensic facial experts are professionals trained to identify faces in images and videos using a set of tools and procedures (10) that vary across forensic laboratories (19). We tested two classes of forensic facial professionals. Examiners ($n = 57$, 28 females, from five continents) have extensive training, and their identity comparisons involve a rigorous and time-consuming process. Their identification decisions can be presented in written documents that can be used to support legal actions, prosecutions, and expert testimony in court. Reviewers ($n = 30$, 17 females, from two continents) are trained to perform faster and less rigorous identifications that may be used in law enforcement and can assist in generating leads in criminal cases. We also tested superrecognizers ($n = 13$, 8 females, from two continents) (20), defined here as a person who had taken a standard face recognition test that qualified them as a superrecognizer (1) or as a person used professionally as a superrecognizer (e.g., the London Metropolitan Police) (*SI Appendix*, *SI Text*).

Fig. 1. Examples highlighting the face region in the images used in this study (all image pairs are shown in *SI Appendix*, Figs. S8–S14). (*Left*) This pair is a same identity pair, and (*Right*) this pair shows a different identity pair.

Professional fingerprint examiners and undergraduate students served as control groups. Fingerprint examiners ($n = 53$, 41 females, from two continents) are trained forensic professionals who perform fingerprint comparisons. They provide a baseline for forensic ability and training that excludes expertise in facial forensics. Fingerprint examiners complete extensive training for professional certification. Undergraduate students ($n = 31$, 24 females, from one continent) were tested as a proxy for the general population.

To compare humans with face recognition algorithms, four DCNNs were tested on the same stimuli judged by humans. We refer to the algorithms as A2015 (14), A2016 (15), A2017a (16), and A2017b (17). The inclusion of multiple algorithms provides a robust sample of the state of the art for automatic face recognition. To make the test comparable with humans as an "unfamiliar" face matching test, we verified that none of the algorithms had been trained on images from the dataset used for the human test. Note that A2015 can be downloaded from the web and therefore, provides a public benchmark algorithm.

Results

Accuracy. Fig. 2 shows performance of the subject groups and algorithms using the area under the receiver operating characteristic curve (AUC) as a measure of accuracy. The groups are ordered by AUC median from the most to least accurate: facial examiners (0.93), facial reviewers (0.87), superrecognizers (0.83), fingerprint examiners (0.76), and students (0.68). Algorithm performance increased monotonically from the oldest algorithm (A2015) to the newest algorithm (A2017b). Comparing the algorithms with the human groups, the publicly available algorithm (A2015) performed at a level similar to the students (0.68). Algorithm A2016 performed at the level of fingerprint examiners (0.76). Algorithm A2017a performed at a level (0.85) comparable with the superrecognizers (0.83) and reviewers (0.87). The performance of A2017b (0.96) was slightly higher than the median of the facial examiners (0.93).

More formally, all face specialist groups surpassed fingerprint examiners (facial examiners, $P = 2.14 \times 10^{-6}$; facial reviewers, $P = 0.004$; superrecognizers, $P = 0.017$). The face specialist groups also surpassed students (facial examiners, $P = 2.53 \times 10^{-8}$; facial reviewers, $P = 4.01 \times 10^{-6}$; superrecognizers, $P = 0.0005$) (*SI Appendix*, *SI Text*). Performance across the face specialist groups did not differ statistically. Summary statistics for accuracy, however, should be interpreted in the context of the full performance distributions within each group.

Performance Distributions. Individual accuracy varied widely in all groups. All face specialist groups (facial examiners, reviewers, and superrecognizers) had at least one participant with an AUC below the median of the students. At the top of the distribution, all but the student group had at least one participant with no errors. To examine specialist groups in the context of the general population (students), we fit a Gaussian distribution to the student AUCs (*SI Appendix*, *SI Text*). Next, we computed the fraction of participants in each group who scored above the 95th percentile (Fig. 2, dashed line). For the facial examiner group, 53% were above the 95th percentile of students; for the facial reviewers, this proportion was 36%. For superrecognizers, it was 46%, and for fingerprint examiners, it was 17%. For the algorithms, the accuracy of A2017b was higher than the majority (73%) of participants in the face specialist groups. Conversely, 35% of examiners, 13% of reviewers, and 23% of superrecognizers were more accurate than A2017b. Compared with students, the accuracy of A2017b was equivalent to a

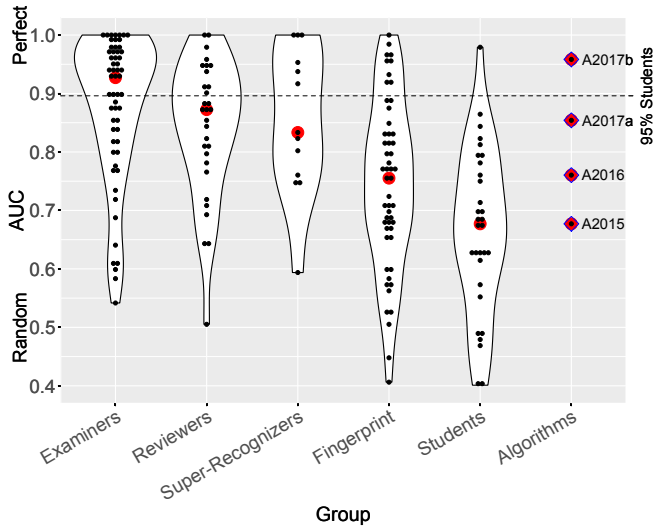


Fig. 2. Human and machine accuracy. Black dots indicate AUCs of individual participants; red dots are group medians. In the algorithms column, red dots indicate algorithm accuracy. Face specialists (facial examiners, facial reviewers, and superrecognizers) surpassed fingerprint examiners, who surpassed the students. The violin plot outlines are estimates of the density for the AUC distribution for the subject groups. The dashed horizontal line marks the accuracy of a 95th percentile student. All algorithms perform in the range of human performance. The best algorithm places slightly above the forensic examiners' median.

student at the 98th percentile (z score = 2.090), A2017a was at the 91st percentile (z score = 1.346), A2016 was at the 76th percentile (z score = 0.676), and A2015 was at the 53rd percentile (z score = 0.082). These results show a steady increase in algorithm accuracy from a level comparable with students in 2015 to a level comparable with the forensic facial examiners in 2017.

Fusing Human Judgments. In forensic practice, it is common for multiple examiners to review an identity comparison to assure consistency and consensus (3, 5). To examine the effects of fusion on accuracy, we combined individual participants' judgments in each group. We began with one participant and increased the number of participants' judgments fused from 2 to 10. To fuse n participants, we selected n participants randomly and averaged their rating-based judgments for each image pair. For fusing judgments, averaging is generally the most effective fusion strategy (21). An AUC was then computed from these average judgments. The sampling procedure was repeated 100 times for each value of n.

Median accuracy peaked at 1.0 (no errors) with the fusion of four examiners or three superrecognizers (Fig. 3). The performance of all of the groups increased with fusion (*SI Appendix*, *SI Text*). For reviewers, the median peaked at 0.98 with 10 participants fused. Fingerprint examiners peaked at a median of 0.97 for 10 participants. For superrecognizers, the median increased from 0.83 to 0.98 when two superrecognizers were fused and to 1.0 when three or more superrecognizers were fused. Using a fusion perspective in comparing accuracy across participant groups, the data indicate that the median examiner (0.93) performs at a level roughly equal to two facial reviewers (median = 0.93) and seven fingerprint examiners (median = 0.94). Notably, the median of individual judgments by examiners is superior to the combination of 10 students (median = 0.88).

Fusing Humans and Machines. We examined the effectiveness of combining examiners, reviewers, and superrecognizers with algorithms. Human judgments were fused with each of the four algorithms as follows. For each face image pair, an algorithm returned a similarity score that is an estimate of how likely it is that the images show the same person. Because the similarity score scales differ across algorithms, we rescaled the scores to the range of human ratings (*SI Appendix*, *SI Text*). For each face pair, the human rating and scaled algorithm score were averaged, and the AUC was computed for each participant–algorithm fusion.

Fig. 4 shows the results of fusing humans and algorithms. The most effective fusion was the fusion of individual facial examiners with algorithm A2017b, which yielded a median AUC score of 1.0. This score was superior to the combination of two facial examiners (Mann–Whitney U test = 2.82×10^4, $n_1 = 1{,}596$, $n_2 = 57$, $P = 8.37 \times 10^{-7}$). Fusing individual examiners with A2017a and A2016 yielded performance equivalent to the fusion of two examiners (Mann–Whitney U test = 4.53×10^4, $n_1 = 1{,}596$, $n_2 = 57$, $P = 0.956$; Mann–Whitney U test = 4.33×10^4, $n_1 = 1{,}596$, $n_2 = 57$, $P = 0.526$, respectively). Fusing one examiner with A2015 did not improve accuracy over a single examiner (Mann–Whitney U test = 1,592, $n_1 = 57$, $n_2 = 57$, $P = 0.86$). Fusing one examiner with A2017b proved more accurate than fusing one examiner with either A2017a or A2016 (Mann–Whitney U test = 1,054, $n_1 = 57$, $n_2 = 57$, $P = 7.92 \times 10^{-4}$; Mann–Whitney U test = 942, $n_1 = 57$, $n_2 = 57$, $P = 7.28 \times 10^{-5}$, respectively). Finally, fusing one examiner with both A2017b and A2017a did not improved accuracy over fusing one examiner with A2017b (Mann–Whitney U test = 1,414, $n_1 = 57$, $n_2 = 57$, $P = 0.21$). This analysis was repeated for fusing algorithms and facial reviewers and for fusing algorithms and superrecognizers. Similar results were found for both groups (*SI Appendix*, *SI Text*).

Error Rates for Highly Confident Decisions

In legal proceedings, the conclusions of greatest impact are identification errors made with high confidence. These can lead to

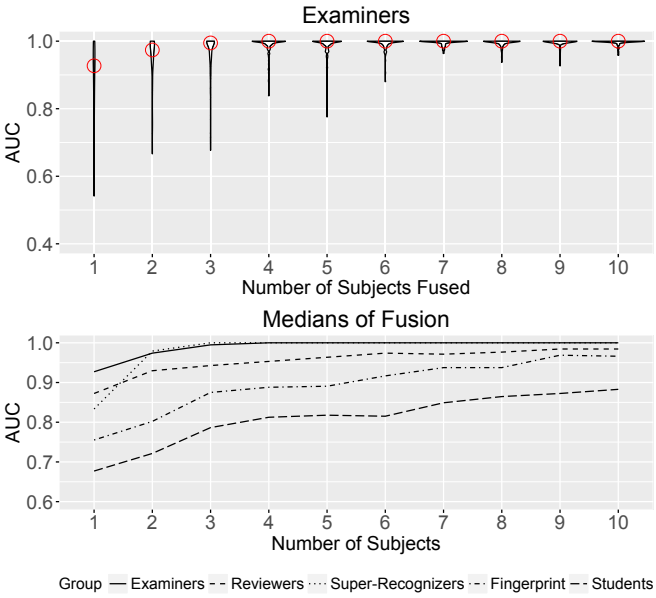


Fig. 3. Plots illustrate the effectiveness of fusing multiple participants within groups. For all groups, combining judgments by simple averaging is effective. The violin plots in *Upper* show the distribution of AUCs for fusing examiners. Red circles indicate median AUCs. In *Lower*, the medians of the AUC distributions for the examiners, reviewers, superrecognizers, fingerprint examiners, and students appear. The median AUC reaches 1.0 for fusing four examiners or fusing three superrecognizers. The median AUC of fusing 10 students was 0.88, substantially below the median AUC for individual examiner accuracy.

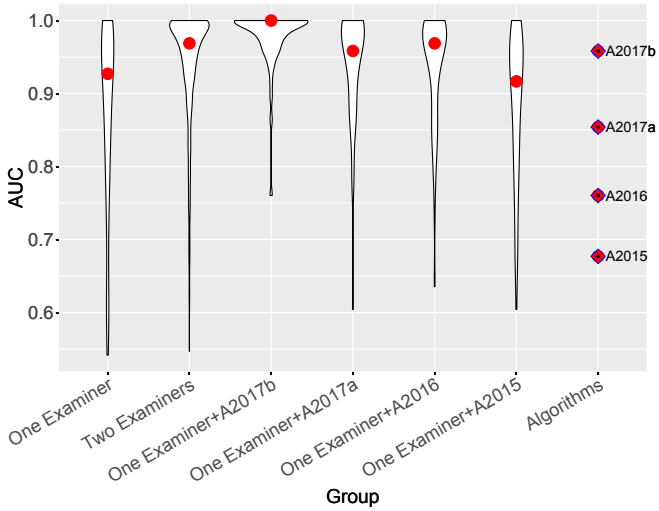


Fig. 4. Fusion of examiners and algorithms. Violin plots show the distribution of AUCs for each fusion test. Red dots indicate median AUCs. The distribution of individual examiners and the fusion of two examiners appear in columns 1 and 2. Also, algorithm performance appears in column 7. In between, plots show the forensic facial examiners fused with each of the four algorithms. Fusing one examiner and A2017b is more accurate than fusing two examiners, fusing examiners and A2017a or A2016 is equivalent to fusing two examiners, and fusing examiners with A2015 does not improve accuracy over a single examiner.

miscarriages of justice with profound societal implications. In this study, the two responses that expressed high confidence were "the observations strongly support that it is the same person" (+3) and "the observations strongly support that it is not the same person" (−3). To examine the error rates associated with judgments of +3 and −3, we computed the fraction of high-confidence same-person (+3) ratings made to different identity face pairs and estimated the error rate as a Bernoulli distribution. The Bernoulli parameter $\hat{q}$ is the fraction of different identity pairs that were given a rating of +3. Fig. 5 shows the estimated parameter $\hat{q}$ with 95% confidence intervals by participant group. (*SI Appendix*, Table S2 shows estimated Bernoulli parameters and the confidence intervals.) The analysis was also conducted on the probability of same identity pairs being assigned a −3 rating.

For facial examiners, the error rate for judging with high confidence that two different faces were the same was 0.009 (upper limit of the confidence interval, 0.022). The corresponding error rate on judging the same person as two different people was 0.018 (upper limit of confidence interval, 0.030). For facial reviewers, the corresponding error rates and confidence intervals were similar to those for the facial examiners (*SI Appendix*, *SI Text*). For superrecognizers, although their error rate for the rating of +3 on two different faces was comparable with that of examiners and reviewers, their error rate for −3 ratings assigned to same face image pairs was higher. Student error rates for high-confidence decisions were substantially higher than those of the facial examiners, reviewers, and superrecognizers. Notably, we found that fusion reduced high-confidence errors for facial examiners, facial reviewers, and superrecognizers (*SI Appendix*, *SI Text*). Specifically, fusing one individual and A2017b was superior to fusing two individuals, and fusing two individuals was superior to one individual.

One possible explanation for these results is that forensic professionals avoid extreme ratings at both ends of the scale. To test this, we examined whether forensic professionals (facial examiners, facial reviewers, fingerprint examiners) overall made fewer high-confidence responses than nonprofessionals (superrecognizers, students). For each participant, the number of high-confidence responses was computed. Analysis showed that forensic professionals made fewer high-confidence decisions than nonforensic professionals (Mann–Whitney U test = 1,966.5, $n_1 = 140$, $n_2 = 44$, $P = 2.83 \times 10^{-4}$). This is consistent with a result obtained in a previous study by Norell et al. (22), which tested police detectives and students on face identity matching experiments. The result suggests that forensic training of any kind may affect the use of the response scale to avoid errors made with high confidence.

Discussion

The results of the study point to tangible ways to maximize face identification accuracy by exploiting the strengths of humans and machines working collaboratively. First, to optimize the accuracy of face identification, the best approach is to combine human and machine expertise. Fusing the most accurate machine with individual forensic facial examiners produced decisions that were more accurate than those arrived at by any pair of human and/or machine judges. This human–machine combination yielded higher accuracy than the fusion of two individual forensic facial examiners. Computational theory indicates that fusing systems works best when their decision strategies differ (21, 23). Therefore, the superiority of human–machine fusion over human–human fusion suggests that humans and machines have different strengths and weaknesses that can be exploited/mitigated by cross-fusion.

Second, for human decisions, the highest possible accuracy is obtained when human judgments are combined by simple averaging. The power of fusing human decisions to improve accuracy is well-known in the face recognition literature (3, 4). Our results speak to the tangible benefits of putting fusion formally into the process of a forensic decision-making process. Collaborative peer review of decisions is a common strategy in facial forensics. This study suggests that, in addition to social collaboration, computationally combining multiple independent decisions made in isolation also produces solid gains in accuracy (24). Although fusing student judgments improves accuracy, we show that there are limits to the gains possible from fusion. A fusion of student judgments will not approach the accuracy of fusing facial examiners or reviewers. This suggests that a strategy for achieving optimal accuracy is to fuse people in the most accurate group of humans.

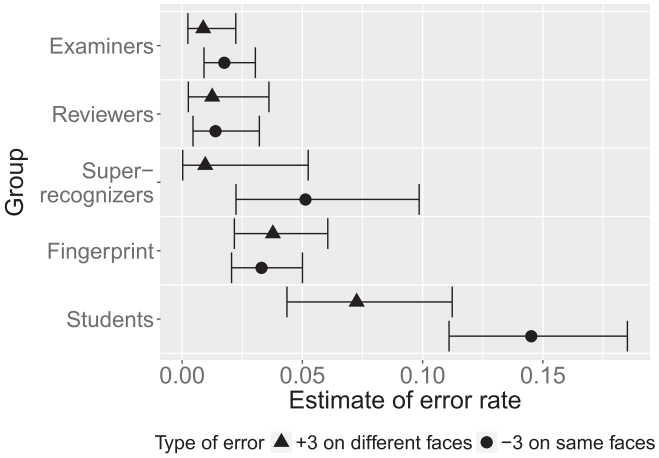


Fig. 5. Estimated probability of highly confident same person ratings (+3 judgment, strong evidence the same person) when the identities are different and estimated probability of highly confident different person ratings (−3 judgment, strong evidence different people) when the identity is the same. The 95% confidence intervals are shown.

Third, systematic differences were found for the performance of the human groups on average. Professional forensic facial examiners, professional facial reviewers, and superrecognizers were the most accurate groups. Fingerprint examiners were less accurate than the face specialists but more accurate than students. Notably, the group medians ranged from highly accurate for facial examiners (AUC = 0.93) to moderately above chance for students (AUC = 0.68). This suggests that our face matching test tapped into the entire operating range of normal human accuracy.

Fourth, the distribution of individual performance in this test was perhaps as informative as the summary data on central tendency. In particular, although the median accuracy measures strongly prescribe the use of professional facial examiners for cases where face identification accuracy is important, some individuals in this group performed poorly. Mitigating this concern to some extent, confident incorrect judgments by facial examiners were extremely rare. At the other end of the spectrum, some individuals in other groups performed with high accuracy that was well within the range of the best face specialists. Remarkably, in all but the student group, at least one individual performed the test with no errors. The range of accuracy of individuals in each group suggests the possibility of prescreening the general population for people with natural ability at face identification. The superrecognizers in our study were not trained formally in face recognition, yet they performed at levels comparable with those of the facial professionals. This suggests that both talent and training may underlie the high accuracy seen in the two groups of facial professionals.

Turning to the performance of the algorithms, the results indicate the potential for machines to contribute beneficially to the forensic process. Accuracy of the publicly available algorithm that we tested (A2015) was at the level of median accuracy of the students—modestly above chance. The other algorithms follow a rapid upward performance trajectory: from parity with a median fingerprint examiner (A2016) to parity with a median superrecognizer (A2017a) and finally, to parity with median forensic facial examiners (A2017b). There is now a decade-long effort to compare the accuracy of face recognition algorithms with humans (6). In the earliest tests (25), the face matching tasks presented relatively controlled images. As these tests progressed, algorithms and humans were compared on progressively more challenging image pairs. In this study, image pairs were selected to be extremely challenging based on both human and algorithm performance. The difficulty of these items for humans was supported by the accuracy of students, who represent a general population of untrained humans. Students performed poorly on these challenging image pairs. All four of the algorithms performed at or above median student performance. Two algorithms performed in the range of the facial specialists, and one algorithm matched the performance of forensic facial examiners.

In summary, this is the most comprehensive examination to date of face identification performance across groups of humans with variable levels of training, experience, talent, and motivation. We compared the accuracy of state-of-the-art face recognition algorithms with humans and show the benefits of a collaborative effort that combines the judgments of humans and machines. The work draws on previous cornerstone findings on human expertise and talent with faces, strategies for fusing human judgments, and computational advances in face recognition. The study provides an evidence-based roadmap for achieving highly accurate face identification. These methods should be extended in future work to test humans and machines on a wider range of face recognition tasks, including recognition across viewpoint and with low-quality images and video as well as recognition of faces from diverse demographic categories.

Materials and Methods

Test Protocol for Human Participants. To allow examiners access to their tools and methods while comparing face images, participants in all conditions, except the untrained student control group, downloaded the pairs of face images and were allowed 3 mo to complete the comparisons. For facial examiners and reviewers, comparisons were completed in their laboratory using their tools and methods. For superrecognizers and fingerprint examiners, the comparisons were done on a computer using tools available on the computer (e.g., image software tools). Students viewed the face pairs presented on a computer monitor one at a time. The size of the images was preset, and it was the same for all images. Pairs remained visible until a response was entered on the keyboard.

For each pair of face images, the participants in all subject groups were required to respond on a 7-point scale: +3, the observations strongly support that it is the same person; +2, the observations support that it is the same person; +1, the observations support to some extent that it is the same person; 0, the observations support neither that it is the same person nor that it is different persons; −1, the observations support to some extent that it is not the same person; −2, the observations support that it is not the same person; −3, the observations strongly support that it is not the same person. The wording was chosen to reflect scales used by forensic examiners in their daily work. A receiver operating characteristic curve and the AUC were computed from the ratings for each subject.

The experimental design was approved by the National Institute of Standards and Technology (NIST) IRB. Data collection procedures for students were approved by the IRB at the University of Texas at Dallas, and all subjects provided consent.

Test Protocol for Algorithms. Algorithms first encoded each face as a compact vector of feature values by processing the image with the trained DCNN. DCNNs consist of multiple layers of simulated neurons that convolute and pool input (face images), feeding the data forward to one or more fully connected layers at the top of the network. The output is a compressed feature vector that represents a face (algorithm A2015 uses 4,096 features, A2016 uses 320 features, and A2017a and A2017b use 512 features). For each image pair in the test, a similarity score was computed between the representations of the two faces. The similarity score is the algorithm's estimate of whether the images show the same person. To avoid response bias, performance was measured by computing an AUC directly from the similarity score distributions for same and different identity pairs, eliminating the need for a threshold. *SI Appendix, SI Text* has details on the algorithms.

Stimuli. Image pairs were chosen carefully in three screening steps. These steps were based on human and algorithm performance (details follow). The goal of the screening process was to select highly challenging image pairs that would test the upper limits of the participants' skills, while avoiding floor effects for the students. The starting point for pair selection was a set of 9,307 images of 507 individuals taken with a Nikon D70 6 megapixel single-lens reflex camera. Images were acquired during a single academic year in indoor and outdoor settings at the University of Notre Dame. Faces were in approximately frontal pose (Fig. 1 shows example pairs).

We screened for identity matching difficulty with a fusion of three top-performing algorithms from an international competition of algorithms [Face Recognition Vendor Test 2006 (FRVT 2006)] (26). Based on the results of the fusion algorithm, the images were stratified into three difficulty levels (27). Image pairs were further pruned using human experimental data. We began with the accuracy of undergraduate students on the two most difficult levels for the algorithm (28, 29). We selected the highest performing 25% of participants and chose the 84 same identity and 84 different identity image pairs that elicited the highest proportion of errors in this group. These pairs formed a stimulus pool of image pairs that were challenging for humans and previous generation face recognition algorithms. A second stimulus pool was created in a similar way but with the goal of finding image pairs on which previous generation algorithms failed systematically. We sampled the stimuli from those used in a recent study that compared human and computer algorithm performance on a special set of image pairs for which machine performance in the FRVT 2006 (26) was 100% incorrect (29). Specifically, similarity scores computed between same identity faces were uniformly lower than those computed for the different identity image pairs. Finally, we implemented a third level of stimulus screening for both stimulus pools. We used performance on an identity matching task with very short (30 s) stimulus presentation times (3) and sorted these stimuli according to difficulty for the forensic examiners from that test.

Discussions with facial examiners before the study indicated that they were willing to compare 20 pairs of images over a 3-mo period. This

allowed them to spend the time that they would normally spend for a forensic comparison. Using the screening described, we chose 12 image pairs from the first stimulus pool and 8 pairs from the second. There were same ($n = 12$) and different identity ($n = 8$) pairs. The slight imbalance eliminated the use of a process of elimination strategy (*SI Appendix, SI Text*).

Data Availability. Deidentified data for facial examiners and reviewers, superrecognizers, and fingerprint examiners can be obtained by signing a data transfer agreement with the NIST. The images are available by license from the University of Notre Dame. Data for the students and algorithms are in Datasets S1 and S2.

ACKNOWLEDGMENTS. Work was funded in part by the Federal Bureau of Investigation (FBI) to the NIST; the Office of the Director of National Intelligence (ODNI), Intelligence Advanced Research Projects Activity (IARPA) via IARPA R&D Contract 2014-14071600012 (to R.C.); Australian Research Council Linkage Projects LP160101523 (to D.W.) and LP130100702 (to D.W.); and National Institute of Justice Grant 2015-IJ-CX-K014 (to A.J.O.). The views and conclusions contained herein should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of the ODNI, the IARPA, or the FBI. The US Government is authorized to reproduce and distribute reprints for governmental purposes notwithstanding any copyright annotation thereon. The identification of any commercial product or trade name does not imply endorsement or recommendation by the NIST.

1. Noyes E, Phillips PJ, O'Toole AJ (2017) What is a super-recogniser? *Face Processing: Systems, Disorders, and Cultural Differences*, eds Bindermann M, Megreya AM (Nova, New York), pp 173–201.
2. White D, Burton AM, Kemp RI, Jenkins R (2013) Crowd effects in unfamiliar face matching. *Appl Cognit Psychol* 27:769–777.
3. White D, Phillips PJ, Hahn CA, Hill MQ, O'Toole AJ (2015) Perceptual expertise in forensic facial image comparison. *Proc R Soc B* 282:20151292.
4. Dowsett AJ, Burton AM (2015) Unfamiliar face matching: Pairs out-perform individuals and provide a route to training. *Br J Psychol* 106:433–445.
5. O'Toole A, Abdi H, Jiang F, Phillips PJ (2007) Fusing face recognition algorithms and humans. *IEEE Trans Syst Man Cybern B* 37:1149–1155.
6. Phillips PJ, O'Toole AJ (2014) Comparison of human and computer performance across face recognition experiments. *Image Vis Comput* 32:74–85.
7. Phillips PJ (2017) A cross benchmark assessment of deep convolutional neural networks for face recognition. *Proceedings of the 12th IEEE International Conference on Automatic Face Gesture Recognition*, pp 705–710. Available at https://ieeexplore.ieee.org/document/7961810/. Accessed May 14, 2018.
8. National Research Council (2009) *Strengthening Forensic Science in the United States: A Path Forward* (National Academies Press, Washington, DC).
9. White D, Norell K, Phillips PJ, O'Toole AJ (2017) Human factors in forensic face identification. *Handbook of Biometrics for Forensic Science*, eds Tistaerlli M, Champod C (Springer, Cham, Switzerland), pp 195–218.
10. Facial Identification Scientific Working Group (2012) Guidelines for facial comparison methods, Version 1.0. Available at https://www.fiswg.org/FISWG_GuidelinesforFacialComparisonMethods_v1.0_2012_02_02.pdf. Accessed May 14, 2018.
11. Davis JP, Lander K, Evans R, Jansari A (2016) Investigating predictors of superior face recognition ability in police super-recognisers. *Appl Cognit Psychol* 30:827–840.
12. Robertson DJ, Noyes E, Dowsett A, Jenkins R, Burton AM (2016) Face recognition by metropolitan police super-recognisers. *PLoS One* 11:e0150036.
13. White D, Dunn JD, Schmid AC, Kemp RI (2015) Error rates in users of automatic face recognition software. *PLoS One* 10:e0139827.
14. Parkhi OM, Vedaldi A, Zisserman A (2015) Deep face recognition. *Proceedings of the British Machine Vision Conference*, eds Xie X, Jones MW, Tam GKL, pp 41.1–41.12. Available at www.bmva.org/bmvc/2015/index.html. Accessed May 14, 2018.
15. Chen JC, Patel VM, Chellappa R (2016) Unconstrained face verification using deep cnn features. *Proceedings of the IEEE Winter Conference of Appl Computer Vis (WACV)*, pp 1–9. Available at https://ieeexplore.ieee.org/document/7477557/. Accessed May 14, 2018.
16. Ranjan R, Sankaranarayanan S, Castillo CD, Chellappa R (2017) An all-in-one convolutional neural network for face analysis. *Proceedings of the 12th IEEE International Conference on Automatic Face Gesture Recognition Gesture Recognition*, pp 17–24. Available at https://ieeexplore.ieee.org/document/7961718/. Accessed May 14, 2018.
17. Ranjan R, Castillo CD, Chellappa R (2017) L2-constrained softmax loss for discriminative face verification. arXiv:170309507.
18. Taigman Y, Yang M, Ranzato M, Wolf L (2014) Deepface: Closing the gap to human-level performance in face verification. *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR)* (IEEE, Washington, DC), pp 1701–1708.
19. Prince J (2012) To examine emerging police use of facial recognition systems and facial image comparison procedures—Israel, Netherlands, UK, USA, Canada. *The Winston Churchill Memorial Trust of Australia*. Available at https://www.churchilltrust.com.au/media/fellows/2012_Prince_Jason.pdf. Accessed May 14, 2018.
20. Russell R, Duchaine B, Nakayama K (2009) Super-recognizers: People with extraordinary face recognition ability. *Psychon Bull Rev* 16:252–257.
21. Kittler J, Hatef M, Duin RPW, Matas J (1998) On combining classifiers. *IEEE Trans Pattern Anal Mach Intell* 20:226–239.
22. Norell K, et al. (2015) The effect of image quality and forensic expertise in facial image comparisons. *J Forensic Sci* 60:331–340.
23. Hu Y, et al. (2017) Person recognition: Qualitative differences in how forensic face examiners and untrained people rely on the face versus the body for identification. *Vis Cognit* 25:492–506.
24. Jeckeln G, Hahn CA, Noyes E, Cavazos JG, O'Toole AJ (March 5, 2018) Wisdom of the social versus non-social crowd in face identification. *Br J Psychol*, 10.1111/bjop.12291.
25. O'Toole AJ, et al. (2007) Face recognition algorithms surpass humans matching faces across changes in illumination. *IEEE Trans Pattern Anal Mach Intell* 29:1642–1646.
26. Phillips PJ, et al. (2010) FRVT 2006 and ICE 2006 large-scale results. *IEEE Trans Pattern Anal Mach Intell* 32:831–846.
27. Phillips PJ, et al. (2011) An introduction to the good, the bad, and the ugly face recognition challenge problem. *Proceedings of the Ninth IEEE International Conference on Automatic Face Gesture Recognition*, pp 346–353. Available at https://ieeexplore.ieee.org/document/5771424/. Accessed May 14, 2018.
28. O'Toole AJ, An X, Dunlop J, Natu V, Phillips PJ (2012) Comparing face recognition algorithms to humans on challenging tasks. *ACM Trans Appl Perception* 9:1–13.
29. Rice A, Phillips PJ, Natu V, An X, O'Toole AJ (2013) Unaware person recognition from the body when face identification fails. *Psychol Sci* 24:2235–2243.

NATIONAL SHERIFFS' ASSOCIATION

Examples of Law Enforcement Uses of Facial Recognition Technology Provided by the National Sheriffs' Association

Iowa

A shooting at the Iowa Department of Public Safety left one person wounded with a serious but non-life-threatening injury. No documentation was found on the victim who refused to give his identity to Des Moines Police Department detectives. Facial recognition was used to determine a possible identity for the subject, which revealed the victim had a nationwide active warrant for narcotics trafficking.

When an unknown male was found deceased in a soybean field with an execution-style shot to the head, law enforcement found no identification at the scene. Using facial recognition, a possible identification of the deceased male was determined which was subsequently confirmed by family members.

1450 Duke St. • Alexandria, VA 22314 • 703.836.7827 phone • 703.683.6541 fax • www.sheriffs.org • nsamail@sheriffs.org

Georgia

A subject claiming to be a truck driver from Athens, Georgia, engaged with an undercover (UC) investigator in Massachusetts believing the investigator was a 14-year-old child. The subject engaged in sexually explicit conversations, sent the (UC) minor pornography, and indicated his interest in traveling to Massachusetts for sex. The subject's Facebook profile was limited and believed to use a fake name. The investigator reached out to an Internet Crimes Against Children (ICAC) affiliate in Georgia for assistance. Analysts submitted the subject's social media profile photo for facial recognition database checks while exhausting other investigative leads and intelligence sources. The first facial recognition result was a match to the subject, who was using his middle name while chatting with the UC investigator. Based upon the lead developed from the facial recognition results, analysts compiled a comprehensive packet on the subject for the Massachusetts investigator.

The remains of a body were found along a fence line behind an apartment complex in Decatur, Georgia. Six hours earlier at 1:30AM, residents of the complex had reported hearing what sounded like an electrical transformer exploding. The deceased's injuries were consistent with a blast or explosion, and fragments of a metal pipe bomb with added shrapnel were also found. The deceased was a white male, 35-45 years of age, 135-145 lbs. with blue eyes. He was wearing all black including a black balaclava and lone-ranger style mask. Only one finger was still intact, and the fingerprint was not on file. A badly damaged cell phone with a SIM card and a second SIM card were found in the shrubs near the body. Record checks on individuals associated with the cellular telephone were provided and video pulled from the surrounding area. Georgia Information Sharing and Analysis Center (GISAC) assisted with conducting facial recognition through the Georgia Department of Driver Services driver's license photo database. Facial recognition yielded a potential match for the deceased. The match had a protective order against him and was previously arrested for stalking his ex-girlfriend, whose residence was 20 yards from the scene of the explosion. The ex-girlfriend was shown a photo of the deceased and confirmed that it was her ex-boyfriend.
https://www.fox5atlanta.com/news/man-found-dead-following-explosion-in-dekalb-county-identified

Michigan

Homicide Investigation
A local police agency in Michigan submitted a social media photo of a potential suspect where the identity of the subject was unknown. The victim of the crime was shot and killed at his campus apartment and the suspect fled the scene. Investigators provided an image from social media of a potential suspect. Facial recognition was used to provide an investigative lead to the investigator. After further investigation, the candidate from the lead was determined to be the homicide suspect. The suspect was charged and later convicted for the homicide.

Child Predator Investigation
A federal law enforcement agency submitted a social media photo to Michigan's Statewide Network of Agency Photos (SNAP) Unit of a subject suspected of soliciting minors online. A facial recognition search returned a viable candidate and the subject in the lead was confirmed as the suspect in the investigation.

Unidentified Deceased Investigation
A county morgue submitted an image to Michigan's Statewide Network of Agency Photos (SNAP) Unit to help identify an unknown deceased female with severe trauma to the face. Trained facial examiners used specialized software to enhance the image to obtain a better gallery of images from a facial recognition search. When the facial recognition search was conducted, a viable candidate returned. The investigative lead was sent to the morgue and was determined to be the correct person. Investigators were able to make a proper death notification to the family.

Criminal Sexual Conduct (CSC) Investigation
A local police agency in Michigan sent out a bulletin asking for assistance in identifying an individual for a Criminal Sexual Conduct (CSC) complaint that occurred at a fraternity house. The Statewide Network of Agency Photos (SNAP) staff contacted the investigating agency and obtained additional photographs of the suspect. Facial recognition developed an investigative lead. The investigator later confirmed the viable candidate in the lead was the correct suspect.

Armed Bank Robbery Investigation
A facial recognition search of an image in relation to an armed bank robbery in Michigan returned a viable candidate. A lead was generated to the requesting detective. After further investigation, the subject in the investigative lead confessed to the armed robbery. Facial recognition was instrumental in expediting the investigation.

Identity Fraud Investigation
While working on identity fraud detection, Michigan's Statewide Network of Agency Photos (SNAP) Unit staff uncovered a potential fraud case when they found a subject whose image appeared on nine different records, each with a different name, with one presumably legitimate. The investigation also revealed the subject had additional alias names and spelling variations. A potential fraud report was turned over to investigators. Without facial recognition, investigators may not have known this subject was potentially victimizing eight different people by using their driver licenses for fraudulent purposes.

Narcotics Trafficking Investigation
The Statewide Network of Agency Photos (SNAP) Unit in Michigan received a request from an out-of-state law enforcement agency to help identify an unknown subject believed to be from Michigan who was part of a drug trafficking ring in their state. A facial recognition search was conducted, and a viable

candidate returned. The investigative lead was provided to investigators who later confirmed this was the subject they were attempting to identify. This subject was involved in numerous drug trafficking investigations in Michigan and West Virginia.

Human Trafficking and Exploitation Investigation
The Statewide Network of Agency Photos (SNAP) Unit in Michigan received a photo of an alleged juvenile victim suspected of being sex trafficked on a popular website known for this type of activity. Facial recognition developed a viable investigative lead. The viable candidate in the lead, a juvenile, was confirmed as being a victim of sex trafficking.

Human Trafficking Investigation
A local Michigan task force requested a facial recognition search on a juvenile female found on a local website known for human trafficking activity. A facial recognition search was performed, and a viable candidate was identified. A lead report with information on the candidate was returned to the agent who confirmed her identity. In a raid on the suspected house where the juvenile was being held, they found the young girl identified through facial recognition as well as five other missing juveniles. The suspect was charged with human trafficking.

Unknown Deceased
A local sheriff's department requested a facial recognition search on an unknown decedent who froze to death in a car. A facial recognition search was conducted revealing a viable candidate. A lead was returned to the deputy and his identity was confirmed to be that of the lead.

Driver Identification
At a traffic stop, a driver did not have identification but provided a name and date of birth. Upon receiving permission from the driver, the law enforcement officer took her photo and ran it through Mobile Facial Recognition to verify her identity. Four mug shots and two previous driver's license images returned. The name and date of birth the driver had provided was her sister's information. The driver was taken into custody and arrested.

Unidentified Deceased
At the scene of a fatal accident, a deceased individual did not have any identification on him. The detective used mobile facial recognition to identify the individual.

Forgery Investigation
Over a three-month period in 2019, facial recognition searches of an individual committing forgery and counterfeiting were requested three times by three different local departments. The Michigan Statewide Network of Agency Photos (SNAP) Unit provided investigative leads to each of these departments and

connected the three departments to assist in their investigations. The suspect that was identified as a viable candidate was formally charged with forgery and counterfeiting.

New York

Rice-cooker bomb suspect identified with help of facial recognition technology (NYC) - 2019
https://nypost.com/2019/08/25/how-nypds-facial-recognition-software-ided-subway-rice-cooker-kook/

Suspect identified with help of facial recognition technology in diamond district gunpoint robbery of $4 million in jewelry - 2019
https://www.nydailynews.com/new-york/nyc-crime/ny-diamond-heist-facial-recognition-20190828-g6fjqkpq3nbshamsd5be4y3nny-story.html

Washington, DC

The Bureau of Alcohol, Tobacco, Firearms and Explosives' (ATF) Washington Field Division needed to identity a suspected firearms trafficker. A trained facial recognition examiner in the National Capital Region worked with photo evidence from a social media account and utilized facial recognition software against regional booking and arrest photos. The examiner provided an investigative lead on the possible suspect to ATF. After further investigation using the lead, the identification was confirmed.

Members of the Metropolitan Police of the District of Columbia (MPDC)/FBI Child Exploitation and Human Trafficking Task Force were attempting to identity a victim being commercially sexually exploited by a known human trafficker. The victim had been physically assaulted by the known trafficker. Working with photo evidence from a surveillance operation, a trained facial recognition examiner used facial recognition software against regional booking and arrest photos to assist MPDC. An investigative lead was provided on the possible suspect. During further investigation, the identification was confirmed.

Members of the MPDC/FBI Child Exploitation and Human Trafficking Task Force assisted in the arrest of a felon in possession of a firearm near an area known for commercial sexual exploitation in Washington, DC. During the arrest, the defendant made statements insinuating he was a pimp/trafficker and that he had recently traveled to Miami, Florida, with two prostitutes. Photographs of the women were located but investigators were unable to identify the women. The photographs were sent to a trained facial recognition examiner who used facial recognition technology to tentatively identify the women and then positively identify the women using corroborating information from other databases. This information was crucial to progress an investigation against a known felon engaged in the criminal sexual exploitation of women.

Maryland

Surveillance video captured an armed carjacking, including images of the suspects and their vehicle. Facial recognition was used on images from the video and provided an investigative lead for one suspect in the video. A query of the subject's name in other databases yielded a recent police encounter in another Maryland county. In the report of that encounter, a detailed description of the subject's vehicle matched the suspect's vehicle from the armed carjacking. This information provided additional evidence that the suspect was the person in the previous encounter.

Virginia

Prince William County (PWC) Police in Virginia received a message for follow-up from a group for veterans regarding Facebook posts by an unknown person stating he did not want to live anymore and was looking into a gun. The veteran group did not know the poster, his real name, or where he lived but sent it to PWC police because there was a link to Dale City. A PWC police department crime analyst used facial recognition software to compare the Facebook poster's image and developed a lead as to who the subject might be. They made contact with the poster and provided help.

Florida

Fugitive Apprehension
In February 2017, a forensic artist was updating age progression images for a 26-year fugitive wanted for participating in a South Florida cocaine trafficking organization. Images of the fugitive were entered into Face Analysis Comparison Examination System (FACES) and the forensic artist saw one potential match was a Florida driver license photograph that strongly resembled the fugitive but with a different name. The information was passed on to federal law enforcement partners and the subject was arrested weeks later. The subject was sentenced to approximately 11 years in federal prison.

Missing Child Investigation
In March 2018, local and federal law enforcement officers were trying to recover a child missing for four months. The child had a history of running away from foster care and falling victim to child sex trafficking. The investigation revealed a Facebook image of an adult male who appeared to be the child's boyfriend. The image was entered into FACES and, among the result was a driver license photograph that strongly resembled the probe image. Further investigation of the individual revealed he was currently on probation. Law enforcement officers initiated surveillance on the subject which revealed the missing child hiding in the rear seat of the subject's vehicle. The missing child was recovered.

Child Sexual Exploitation Investigation
In 2017, detectives were conducting online undercover investigations related to child sexual exploitation. An undercover officer posted online while posing as a 14-year-old girl. An adult male who said he was in his thirties responded to this post. He continued conversation with someone he believed to be a 14-year-old girl despite being informed repeatedly of "her" age. The male provided a photograph of himself which was processed through FACES. Among the results was a driver license photograph which strongly resembled the probe image. Further investigation ultimately led to the location and arrest of the subject for multiple felony charges related to the online seduction of a minor.

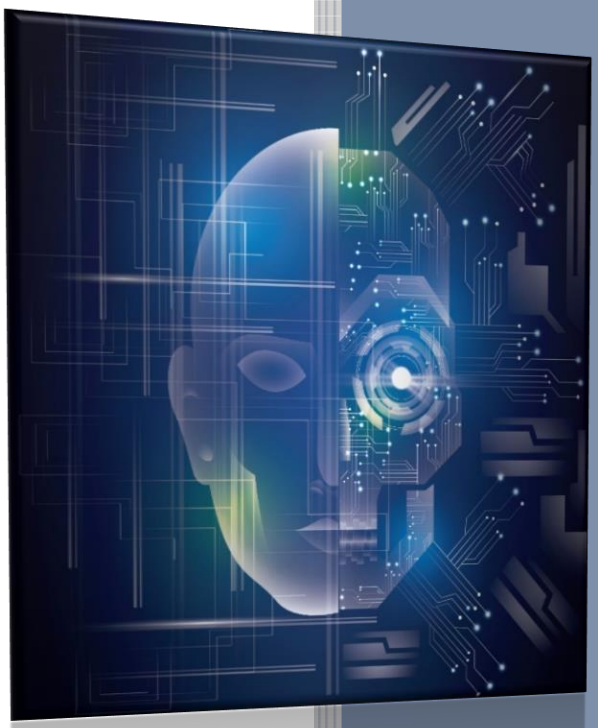
Missing Person Investigation
In February 2010, law enforcement officers were investigating a runaway case involving a juvenile female. During the investigation, social media images were obtained of an unknown subject believed to be harboring the juvenile runaway. Images were enrolled into FACES and searched. A potential match was found, and the identity was verified. The detectives determined the suspect's location, recovered the runaway juvenile, and made an arrest of the suspect for harboring a runaway.

Fraud Investigation
In September 2018, a male suspect attempted to rent a high-end vehicle by using a fraudulent Kansas driver license. The rental car employee was suspicious of the male and took a photograph of the driver license. The suspect took the driver license and fled the business. Detectives processed the photograph of the fraudulent driver license through FACES and found a potential match. Additional investigation revealed the suspect was on probation. The probation officer confirmed the suspect was indeed her probationer. An arrest warrant was issued for felony charges and Violation of Probation.

Domestic Battery Investigation
In February 2019, officers were dispatched to a domestic battery call where the male fled on his bike. When officers located him, he was not cooperative. The male provided a name to the officers that could not be confirmed. Officers obtained a photograph of the subject and searched FACES. A prior booking photograph from a neighboring county resembled the subject. The male confirmed that he was the individual officers suspected him to be following the facial recognition search. Further investigation revealed the subject had outstanding arrest warrants for seven charges from a nearby county and he was arrested.

IJIS Institute

LAW ENFORCEMENT FACIAL RECOGNITION USE CASE CATALOG



Law Enforcement Imaging Technology Task Force

A joint effort of the IJIS Institute and the International Association of Chiefs of Police

March 2019

ACKNOWLEDGEMENTS

The IJIS Institute and the International Association of Chiefs of Police (IACP) would like to thank the following contributors for supporting the creation of this document:

Contributors

- Patrick Doyle – LEITTF Co-Chair and New Jersey State Police, Lieutenant (Ret.)
- Bonnie Locke – LEITTF Co-Chair and Nlets Business Development Director
- Jamie Algatt – Senior Product Manager, RapidDeploy USA
- Steve Ambrosini – Program Director, IJIS Institute
- Ben Bawden – Partner, Brooks Bawden Moore LLC Consultants
- Maria Cardiellos – Director of Operations, IJIS Institute
- Robert E. Greeves – Senior Policy Advisor, National Criminal Justice Association
- Pete Fagan – Virginia State Police, Lieutenant (Ret.)
- Jenner Holden – Chief Information Security Officer, Axon
- Robert May – Program Director, IJIS Institute
- James Medford – USAF Lt. Col. (Ret.)
- Catherine Miller – National Capital Region NCR-LInX Program Manager
- Dave Russell – Director, Northern Virginia Regional Identification System
- Pam Scanlon – IACP CJIS Committee Chair and Director, ARJIS/San Diego
- David M. Shipley – Executive Director, Colorado Information Sharing Consortium
- Robert Turner – President, CommSys Incorporated
- Gerald L. Ward, Ph.D. – MTG Management Consultants, LLC
- Heather Whitton – Cincinnati Police License Plate Reader Program Manager

EXECUTIVE SUMMARY

This Law Enforcement Facial Recognition Use Case Catalog is a joint effort by a Task Force comprised of IJIS Institute and International Association of Chiefs of Police. The document includes a brief description of how facial recognition works, followed by a short explanation of typical system use parameters. The main body of the catalog contains descriptions and examples of known law enforcement facial recognition use cases. A conclusion section completes this catalog, including four recommended actions for law enforcement leaders.

TABLE OF CONTENTS

FOREWARD

Police work is constantly adapting to an ever-changing environment, yet it has always been grounded in one simple, founding principle – to make the world a safer place.

To that end, law enforcement agencies, and other public safety entities must not only stay abreast of the latest tactics and technologies used by criminals, but also deploy every available method to maintain order, thwart wrongdoing, and ensure that those who threaten the peace are held accountable for their actions – all while respecting the rights of those involved.

However, new police technologies and procedures do not automatically coincide with new laws, rules, or policies governing their use. Their initial deployment can sometimes be misunderstood, and, in some cases, technological capabilities in the hands of law enforcement can exceed the public's comfort level. It can take some time before both citizens and the courts widely accept high-tech police tools. Such a learning curve and adjustment period has occurred with everything from issuance of police firearms to traffic radar speed monitoring devices.

What is unknown is often feared – or at least misunderstood – sometimes leading to overreactions and overreaching by policy makers. This response can limit the extraordinary new ways these advances can help ensure public safety.

Today, law enforcement is wrestling with similar issues in the case of facial recognition, which is sometimes referred to as facial analysis or face matching. Facial recognition is a remarkable development that helps law enforcement exonerate the innocent, narrow searches for the guilty, and otherwise maximize limited resources. Simply put, it greatly expedites certain police functions through the rapid comparison of one facial image to many others.

While the term *facial recognition* has become somewhat synonymous in the media and among other stakeholder groups to describe all uses of this technology, such systems used by law enforcement provide recognition of *potential* candidates, not recognition of *exact* matches as the name might insinuate. Law enforcement best practices for all known use cases still requires a human examiner to confirm that one of the computer-provided candidates matches the submitted image. The computer or software system does not make the final decision regarding an exact match when proper police procedures are being followed – a trained person does.

Public safety professionals use facial recognition in various ways to help them discover or find individuals, and to assist with the identification of people. But, because facial recognition uses the very personal and particular attributes within an image of the human face, it has a very private and individual connotation to it. The fact that it can help sort through great volumes of images, and that citizens aren't necessarily aware their own faces are in such comparative databases, only heighten the potential anxiety over the use of facial recognition technologies. These issues, have created an environment where something as promising as facial recognition has the potential to be viewed as a problem itself, rather than an answer to one.

What appears to be immediately needed is a balanced and well-informed approach to facial recognition by law enforcement, which will help ensure public understanding of the way in which the technology is used by law enforcement, and to what end.

PURPOSE OF THIS CATALOG

The IJIS Institute and the International Association of Chiefs of Police (IACP) are both research entities and policy development bodies, but each has different core memberships. The combination of these two groups into a task force provides a multi-faceted perspective to technology issues. IJIS is a nonprofit alliance of industry representatives, technology developers, practitioners, national associations, and academic organizations, while IACP is comprised largely of justice leaders and law enforcement practitioners, the blend of experience and competencies between these organizations is a desired benefit in this catalog.

With a combined global membership of more than 31,000, IJIS and IACP together have deep knowledge, academic prowess, and practical experience to investigate emerging issues and technologies. The organizations have created a joint research effort known as the Law Enforcement Imaging Technology Task Force (LEITTF) to review emerging trends and technologies such as facial recognition.

The LEITTF has created this document as a catalog of facial recognition use cases for criminal justice agencies, which includes uses by police officers, sheriff's deputies, investigators, and supporting personnel wherever they exist. This examination of uses covers typical settings wherever law enforcement interacts with persons such as large venues, transportation hubs, correctional facilities, motor vehicle stops, crime scenes, and other everyday situations.

The intention of this effort is to briefly describe facial recognition systems and their parameters, determine the ways in which facial recognition is being used, and, most importantly, to document cases which demonstrate the technology's ability to protect the public. The objective is to empower public safety practitioners and industry innovators to communicate the ability of facial recognition to policy makers and the public, while reducing misunderstanding and minimizing the potential for misuse.

The LEITTF has chosen to catalog and explain facial recognition use cases (as opposed to creating model policy, conducting a scientific analysis, or examining other elements of facial recognition) in order to fulfill an immediate need to improve visibility into how these systems are used. Providing real examples from the field further strengthens the context of facial recognition usage so that those outside of law enforcement can appreciate its necessity. It is hoped such details will help encourage outreach from police to concerned citizen groups and, in general, establish a better understanding of facial recognition. Describing the way in which facial recognition is successfully deployed should increase awareness and alleviate at least some of the public's concerns, and perhaps spur healthy discussion into the benefits of using this technology. As has been proven with every successful deployment of technology and law enforcement effort to combat crime, "you cannot police a community without effectively working with that community."[1]

HOW DOES FACIAL RECOGNITION WORK?

Facial recognition has been in limited use for many years. Recent improvements in system accuracy combined with higher demands for biometric identification capabilities have led to more widespread use in private industry such as corporate settings, with public and law enforcement use lagging slightly behind but certainly on the rise.

A typical facial recognition system uses the layout of a subject's facial features, and their relative distance from one another, for identification comparison against a separate image, or perhaps even against thousands or even millions of separate images in a database or gallery of faces. The subject's facial image attributes are derived from either a still or video image – physical presence is not always required.

Computer algorithms then measure the differences between the face being searched and the enrolled faces in a chosen gallery, such as a government database of images. The smaller the differences between the faces considered, the more likely those faces will be recognized and presented as potential matches. Through statistical analysis of the differences, a facial recognition system can provide a list of candidates from the gallery and rate the most likely matches to the image of the subject's face. Using suggested law enforcement best practices (see Summary Recommendation # 4), a trained face examiner would then make the final selection, potentially determining one of the candidates is very likely a match to the original submission. Of course, some facial recognition searches result in no high-probability match candidates. Even if the computer algorithm does return potential match candidates, it is possible, and, in fact, common, that the trained human examiner does not agree, nor does he or she select any candidate as a likely match.

Perhaps the most important element regarding the use of facial recognition by law enforcement is not within the technology itself, but what follows once the computer has suggested candidates and the human examiner determines a likely match exists in a particular case. It is at this point that the police have a strong clue, and nothing more, which must then be corroborated against other facts and investigative findings before a person can be determined to be the subject whose identity is being sought. Therefore, a candidate match, even after confirmation by a trained user, is, in most jurisdictions, not enough evidence for police to detain or arrest a person. All facts, and the totality of circumstances regarding the investigation or search, should be considered before any action is taken.

[1] William Bratton, former NYPD and Boston Police Commissioner, and LAPD Chief.

Facial Recognition Use Types

Facial recognition technology is broadly used in two different sorts of law enforcement situations:

Identify	It can help **identify** a subject face against a known image. For example, this would help confirm that a person's face matches to the digital image of a face embedded in a document presented to law enforcement, such as a passport. This is sometimes known as **one-to-one analysis**, since facial recognition is being asked to provide guidance on whether one submitted sample image is likely the same person as in another image.
Discovery	Facial recognition technology can also help compare the image of a face to numerous known faces within an array or database. For example, this helps police use technology to suggest if a criminal or terrorist in a surveillance video or still image may match any mug shot photos of people previously arrested or convicted. This function is typically called **discovery** and is sometimes referred to as a **one-to-many analysis** since it seeks to compare one image to multiple other images to find candidates for potential matching.

Facial Recognition System Parameters

There are several elements of a facial recognition system which are somewhat similar to other database-reliant technologies. For instance, digital fingerprint systems retain a repository of collected prints, and in many cases, newly submitted prints are often compared to those in the database to see if there are potential prints which may match the sample. It is also possible to compare one set of collected prints to another collected set or print, such as from a crime scene. Facial recognition is often used in similar ways – comparing one-to-one, or comparing-one-to-many. However, there are several distinct differences. For instance, facial recognition is currently somewhat unregulated by laws, policies, and practices regarding image capture, usage, retention, accuracy, and human oversight.

Also, face images can be collected much more easily than fingerprints, sometimes without the person knowing an image of their face has been captured. Most people that are fingerprinted have either consented to prints being taken or have been arrested and have no choice. Face images are sometimes collected with consent, such as with a driver's license photo, but an extended or implied consent over its future use in a repository is not usually given. In some cases, governments prohibit implied consent or do not allow the agency capturing the original photo to even ask for it.

However, in some regions, consent to capture the photo for one purpose does not always expressly prohibit its use by law enforcement. Therefore, some police agencies may use captured images without a person's implied consent.

These types of image captures, uses, and retentions, and the lack of consistent laws or rules throughout many states, provinces, territories, and countries, have helped cause misunderstandings and some resistance to facial recognition systems.

Facial recognition accuracy is also an unsettled discussion in many regions. This technology is without question much more efficient at scanning through large numbers of photos to find potential candidates than could be scanned by manual human comparison, but there are questions about whether the faster, technological approach can ever be 100% accurate.

Some facial recognition research, such as the Georgetown Center for Privacy and Technology Report,[2] have widened the gap between supporters and detractors through suggestions that the systems are at least partially biased toward minorities, and because of such inherent risks, should only be used by police to find very serious criminals. Other recent studies, such as the latest reports by Massachusetts Institute of Technology's (MIT) Computer Science and Artificial Intelligence Lab[3] and IBM,[4] each suggest facial recognition bias can be mitigated through improvements in algorithmic structure, more racially inclusive data sets, and broader facial data point collection. Greater overall independent study is needed, and transparency regarding the results will be essential to maintain public confidence in the technology as the science is refined and fear is mitigated.

There are also media and watchdog group assertions that the technology is in some cases being used to single out a person based *only* upon a computer-driven algorithm's decision, without any significant amount of human oversight to the process. Many of these anecdotal complaints involve alleged use cases where denial of entry or services is the result, such as admission to a sports stadium, *not* detention, arrest or formal criminal prosecution. However, any alleged decision by law enforcement personnel reportedly made solely by facial recognition software, no matter how inconsequential the decision may seem, is alarming to some stakeholder groups. Media reports of this alleged facial recognition usage certainly have stirred criticism, which is also to some degree fueled by reported accuracy improvements made by technology providers. Some media reports allege law enforcement agencies are relying on greater system accuracy to select matching candidates, and less on trained facial recognition human examiners. However, police agencies can avoid such criticism by ensuring facial recognition systems are supported by strong policy, training standards, and human oversight, regardless of increasing accuracy, especially when criminal investigations are being conducted or other impactful actions may be taken which affect the public.

---

[2] Georgetown Law School Center for Privacy and Technology Report, *The Perpetual Line-Up*, October 2016 https://www.perpetuallineup.org/.

[3] Massachusetts Institute of Technology Computer Science and Artificial Intelligence Laboratory Study, *Uncovering and Mitigating Algorithmic Bias Through Learned Latent Structure*, January 2019, http://www.aies-conference.com/wp-content/papers/main/AIES-19_paper_220.pdf.

[4] IBM Corporation, *Diversity in Faces Study*, January 2019, https://www.ibm.com/blogs/research/2019/01/diversity-in-faces/.

Typical Elements of Facial Recognition System Deployments

Facial recognition systems generally involve five significant elements or activities:

1. Image Capture	2. Image Usage	3. Image Retention	4. Image Accuracy	5. Human Oversight
• Usually digital photographs, video stills, etc.	• Predicates for using images held in databases	• The length of time images are kept on file	• Both the quality of the images and the exactness of matching	• The degree to which a person makes actionable decisions

These five aspects each have important variables, leading to potentially different best practices, policies, laws, limitations, and concerns depending on the exact use cases.

Here are the five system aspects listed again, with potential questions about usage parameters following each that law enforcement users may be asked and be prepared to answer:

Image Capture	Who captured the image? When was it captured? How was it captured? Why was it captured? Was consent given to capture it?
Image Usage	Who will use the image? When will it be used? How will it be used? Why will it be used? Will consent be given each time it is used?
Image Retention	Who has the right to retain the image? When do they have the right to retain it? How will it be retained? How long will it be retained?
Image Accuracy	Are image quality, capture, and comparison methods standardized? Are both sample and gallery images similarly standardized? Are accuracy errors random or patterned by sex, race, skin color, affliction, style choices, image accuracy, etc.?
Human Oversight	Are trained examiners the ultimate decision makers? Are examiners trained to certain standards? How often?

Some of these questions may each be answered differently, depending on how facial recognition is being used at the moment, and under what pretenses, and by which type of agency. That is why this catalog presents the following actual known law enforcement use cases of facial recognition systems. These use cases should provide context as to why the public's opinion of this technology may be quite different depending on the actual circumstances of its use and may further depend on the timing of such police use within the justice continuum. What is publicly acceptable for law enforcement to use when detaining known criminals or investigating crimes may not be tolerable for those situations where police are conducting broad surveillance, or routinely patrolling neighborhoods. Examination of law enforcement facial recognition uses cases may help both the police and the public come to terms with how this technology is, and should be, deployed.

USE CASES

Police officers are generally very adaptive and ingenious. The nature of protecting the public usually requires quick-thinking, and the use of things which may go beyond their original intended design is sometimes a necessity.

Such is the case with facial recognition, which was originally intended as a specific investigative tool to help narrow the field of suspects down to a manageable amount. However, law enforcement professionals quickly learned to deploy it as a means of exonerating the falsely accused, identifying the mentally ill, helping return children to their parents, and determining the identity of deceased persons, in addition to other innovative uses.

This Task Force found 19 known uses of facial recognition for law enforcement.
These uses involve both overt, and covert, facial image capture and observation techniques.

Law Enforcement Facial Recognition Use Case Categories

The different ways in which this technology is being used generally fit into three different groupings, based upon the activity or required tasks of the law enforcement professional using facial recognition:

1. Field Use
2. Investigative Use
3. Custodial and Supervisory Use

Many of the 19 uses can also be performed with two distinctly different intentions:

- **Discovery** – helping to find one person among many persons
  (One-to-Many Comparison)
- **Identification** – helping to verify one person is in fact the person being helped or sought
  (One-to-One Comparison)

The database of comparative photos use in each use case can also differ. For example, some law enforcement agencies may use images from public sources (such as department of corrections records) to compare with a recently captured image of a suspect. Other police departments may also use, with appropriate legal authority, a privately-owned gallery, such as one maintained by a sports venue security firm, which, for example, may have been created from video surveillance or ticket-use photo identification databases.

Therefore, each use case may have several variables, such as the intended outcome to either *discover* a person, or *identify* a person, plus be conducted using comparison to either public and private sources of photos, or both, and at different points in an investigation or inquiry into a matter brought to the attention of police, Figure 1.

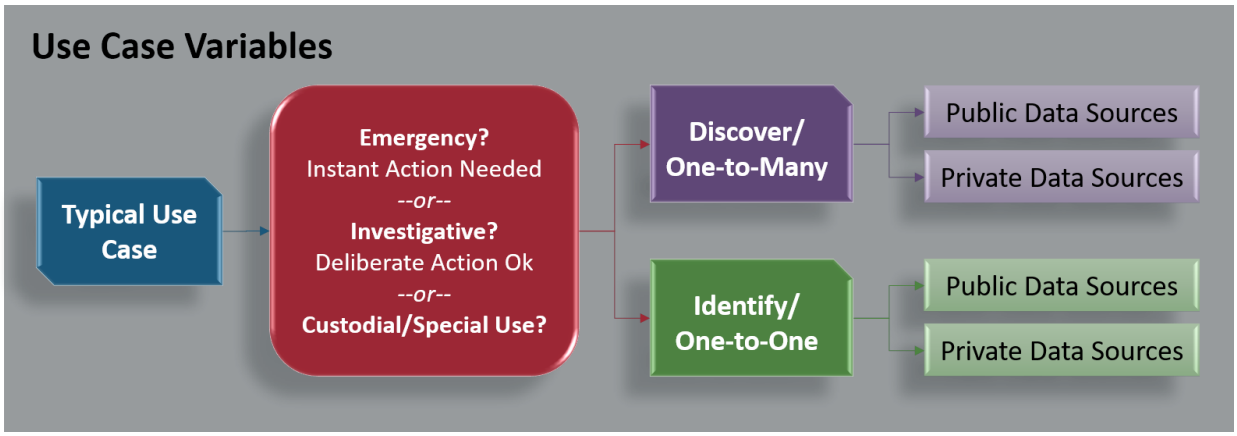


Figure 1

In the following use case descriptions, actual instances or example scenarios follow each use case to further clarify the ways in which facial recognition may be used by law enforcement.

Field Use

The following situations generally occur where an officer uses facial recognition to help positively identify an individual during a face-to-face interaction, or during some other active, uniformed-police response to an incident.

Random Field Interaction

An officer on patrol in the field may be alerted that an individual's image actively captured on an operating in-car or body worn camera may be a possible candidate for a match to a subject in a wanted persons image database.

Example Scenario
Police officers assigned to foot patrol in a business district may be required to operate their body worn cameras during all substantive interactions with the public. During such patrol duties they are often interact with citizens at which time face images captured via activated body worn camera footage may be compared in near real time to a criminal warrants database of fugitive images.

Reasonable Suspicion Interaction

An officer may be alerted to unusual or furtive activity by a person, which presents reasonable suspicion to capture an image of the individual to protect the officer's safety, or to potentially explain the suspicious activity.

Actual Instance - Fugitive Apprehended

In January 2017, an officer assigned to a fugitive task force observed a transient male that matched the description of a known wanted subject. The male was uncooperative and refused to identify himself. The officer captured a photograph of the subject and used facial recognition as one tool to help identify him. The officer then queried NCIC and was informed that the subject had an active felony warrant. He was booked and the case was closed.[5]

Active Incident

During an active criminal situation, video or pictures obtained by officers could be used to potentially help identify individuals and guide active response efforts.

Example Scenario

A situation might occur where a field officer records video of a person's face, such as with an in-car or body worn camera system, and the person then flees the scene of the encounter. Facial recognition could be used to compare the recorded image of the person's face against a database to help determine who the person might be, or why they fled.

Deceased Identification

Deceased individuals can be more quickly identified in the field with facial recognition systems providing possible matched images to a captured imaged of the victim.

Actual Instance - Facial Recognition Used to ID murder victim

Police received a 9-1-1 call of a male subject lying in the street. Officers arrived and located an obviously deceased adult male victim in the roadway. There was evidence of trauma to the victim's body and it would eventually be learned that a homicide had occurred. The victim did not appear to possess any identification and responding detectives were initially unable to identify the subject. A photograph was taken at the crime scene and submitted through a facial recognition program. Within minutes, a candidate photograph was returned, helping to identify the victim as 21-year-old male. This identification was corroborated by other facts obtained in the early stages of the investigation. The speedy identification of the unknown victim in this case was a huge benefit, making it possible for timely notification to the family, and moving the investigation forward towards its eventual resolution through the arrest of two suspects.[6]

[5]Automated Regional Justice Information System, San Diego, California.
[6]Automated Regional Justice Information System, San Diego, California.

Lost & Missing

Lost children or missing adults could be located and identified when encountered by officers during interactions, whereby facial recognition is used to help provide clues to determine identity.

Example Scenario

A situation might occur where a field officer encounters a lost child or disoriented adult and captures an image of the person's face for comparison with a database of lost or missing persons to help identify them.

Interdiction

An individual of interest who is actively avoiding identification can potentially be located at a checkpoint, with facial recognition providing clues for officers to investigate.

Actual Instance - Illegal Alien Attempts Entry

In August 2018, a 26-year-old man traveling from Brazil entered Washington Dulles International Airport and presented agents with a French passport. Agents used facial recognition to compare his passport photo to a database of known images with identities and were alerted that the man's photo might not be a match to his stated identity. The man became nervous when agents referred him for a secondary search. The agents discovered the man's real identification card in his shoe, and it was revealed he hailed from the Republic of Congo. Charges are pending.[7]

Identify Fraud

Incidents often occur where a person presents identification documents to fraudulently obtain access or services, benefits, or credit privileges, and facial recognition can be used to alert officers to possible mismatches.

Actual Instance - Credit Card Fraud

An unknown female pictured in surveillance photos entered a costume store attempting to purchase multiple wigs with a credit card that was stolen from a vehicle earlier in the day. The transactions could not be completed as the cardholder had already canceled the stolen cards. At this time, it is unknown whether the pictured female was also involved in the vehicle trespass. The female was described as having a heavier-set build and dark, shoulder length hair. Checking the surveillance photos against a correctional mug shot database with the agency's facial recognition application revealed the identity of a high-probability candidate, who is now under investigation for use of the stolen credit card.[8]

Actual Instance – Retail Fraud

On March 5, 2018, investigators opened a case involving fraud and the use of counterfeit traveler's checks ranging from $5,000 to $20,000 in multiple jurisdictions. A male and female

[7]United States Customs and Border Protection.
[8]Arapahoe County, Colorado Sheriff's Department.

suspect had opened a membership at a Costco and began using the checks as payment. The investigating agency submitted the new member photos to a facial recognition application and investigators were able to locate candidates in the system and eventually confirm the identities of both suspects. Charges are pending.[9]

Actual Instance - Retail Fraud and Theft

Around April 13, 2018, investigators received an Asset Protection Alert from a local Home Depot not in their jurisdiction. The suspects in these cases have stolen over $5,000.00 in tools from Home Depot stores in nine separate cases and five different stores. The investigator used the agency facial recognition application to compare surveillance photos of the suspect with photos from a correctional mug shot database. The application returned a high-probability candidate now under investigation by Home Depot retail crime investigators and local authorities. Charges are pending.[10]

Actual Instance - Retail Fraud

On June 20, 2018, investigators received a bulletin advising that a suspect has committed two high-dollar thefts at The Home Depot. The suspect was targeting Milwaukee power tools. Total loss for the two cases $1,097.00. Surveillance photographs were entered into the agency's facial recognition application used to search the correctional mug shot database. The application identified two high-probability candidates that additional investigation confirmed were the involved suspects and resulted in recovery of the stolen tools and pending charges.[11]

Investigative

The following use cases generally involve law enforcement using facial recognition technologies to assist in solving crimes, such as use to gather evidence or aid in investigations.

Active Incident

During an active criminal situation, surveillance video can be used to provide images of suspicious persons which may help to identify suspects or witnesses, thereby guiding active response efforts.

Example Scenario

A situation might occur where a terrorist attack is made, and surveillance video of the area prior to the event is obtained. Images of suspicious persons in the video can be entered into other monitoring systems, which can then search for potential matches among other video feeds.

[9]Arapahoe County, Colorado Sheriff's Department.
[10]Arapahoe County, Colorado Sheriff's Department.
[11]Arapahoe County, Colorado Sheriff's Department.

Photo Array Construction

The creation of photo arrays can be automated using an existing suspect photo along with other biometrics information to find similar photos, thereby creating a photo array to be shown to a witness or victim for suspect identification.

Actual Instance - Armed Robbery Suspect Apprehended

An Indiana detective used facial recognition software to help identify a convicted serial robber as the alleged stickup man of a payday loan business. The business' cashiers told police the suspect ran around the counter and flashed a firearm before ordering them to empty two cash registers. Records show that the suspect ordered a cashier to open the store's safe but fled after he noticed a customer walking out of the business on her cellphone. The suspect's face was visible on the store's surveillance footage. Police released footage of the suspect the week after the robbery, but no leads were developed.

A detective then turned to the department's facial recognition software and put a photo of the suspect from the surveillance footage into the system which came up as a possible match. The detective showed the cashiers a photo array, which included the suspect's photo, and they identified him as the robber. The suspect had absconded from parole earlier in Illinois after serving part of a 12-year prison sentence for a string of armed robberies in the northwest Chicago suburbs, according to Illinois Department of Corrections records. He had committed nine robberies over the course of the prior 7 years.[12]

Actual Instance - Sexual Assault Suspect Apprehended

A 15-year old girl was sexually assaulted by an adult male she met online. The girl was only able to provide suspect personal information from his online profile but had also obviously met him in person, so she was familiar with what he looked like in real life and had access to online images of him. Police were able to use facial recognition on one of the digital images, which when compared to DMV photos, provided some candidates from which the girl was able to select a match. Authorities obtained a search warrant for the home of the identified suspect, who later admitted to the crime.[13]

Evidence Compilation

Photos of a known suspect can be used to search across existing traditional photo databases, or even situation-specific databases created from voluntary submissions, surveillance videos, or social media, yielding possible candidates which may match the suspect.

Actual Instance – Jewelry Thief Apprehended Via CrimeStoppers Comparison

On November 3, 2017, an unknown subject was caught on surveillance video at a Jeweler store, taking control over eight gold rings worth $2,000. The Hamilton County Sheriff's Office was asked to assist with the investigation and was in the process of testing its new facial recognition system. Deputies decided to use the jewelry investigation request as a training exercise. They used to publicly-submit CrimeStoppers photos to learn how to analyze the jewelry suspect image

[12]Munster, Indiana Police Department.
[13]Scranton, Pennsylvania Police Department.

to a candidate pool of images and were surprised that after just a dozen or so photos were compared, a strong candidate for a match was found. Detectives took this legitimate lead and started working with investigators from the jurisdiction where the CrimeStoppers submission was made, piecing together the true identity of the suspect. The thief's identity was determined, and he was located and arrested for the jewelry theft, the CrimeStoppers Case and four other outstanding felony warrants.[14]

Actual Instance - Social Media Photo Helps Identify Suspect

A woman was victimized by a stranger whom she met on a dating website. The perpetrator's name and other personal information on his social network page were intentionally deceptive, but the photograph was genuine because his intent was to eventually meet the victim in person. Biometric search of the dating website profile photograph produced a possible match, which after further investigation, led to an arrest.[15]

Actual Instance - Suspect Misidentifies Sex to Avoid Arrest

A police officer used a facial recognition application to help identify a girl who was pretending to be a guy (Justin) instead of a female (Jamie), all to avoid being arrested on a warrant. No record came up on names and DOBs. Field officers used the available facial recognition application by snapping a photo of her in disguise and comparing it to the 4+ million booking photographs in the system. The suspect's FEMALE photograph returned as the #3 candidate. Immediate action on the returned information exposed the disguise and resulted in an arrest.[16]

Actual Instance - Shooting Suspect Identified

On October 17, 2018, a suspect identified by a witness as a tattoo artist and recently-released inmate, known only by the monikers Dough Boy *or* Dough Blow, *shot and seriously injured another person. Using information developed through a bulletin and photos from social media posts made by the suspect, the agency facial recognition application returned a high-probability candidate from a mug shot database. Further investigation revealed a high-probability candidate that the continuing investigation confirmed as the suspect in the shooting. The investigation continues.*[17]

Participant Party Identification

Facial recognition can be used to help confirm a witness, victim, or perpetrator was at a specific crime scene, or associates with a specific suspect or group.

Actual Instance – CCTV Helps Confirm Suspect was at Crime Scene

A crime occurred in view of a local CCTV camera system, and recorded video captured an image of a potential perpetrator's face. Facial recognition was used to compare the image to a photo database, which produced two potential suspects. Further investigation by detectives

[14] Springfield Twp. Police and Hamilton County Sheriff's Office, Ohio.
[15] Safran MorphoTrust Corporation.
[16] Lakewood, Colorado Police Department/Colorado Information Sharing Consortium.
[17] Denver, Colorado Police Department.

in the field helped confirm one of the suspects was at the scene, ultimately leading to his arrest for the crime.[18]

Victims Identification

Facial recognition can assist in potentially identifying victims of crimes, in situations where traditional methods of identification are not available.

Example Scenario

A situation might occur where a victim of a crime appears in a videotape or photograph, such as with a teenager being used in sexually explicit materials, but no report of crime is made to police by the victim or his/her guardians. The image of the victim can be used to search available databases for potentials candidates to be identified.

Criminal Identification

During the monitoring of high risk transit locations, areas of persistent criminal activity or other high-risk locations, images of known wanted persons can be compared against images captured on surveillance video to help locate potential matches.

Example Scenario

A situation might occur where a defiant trespasser or registered sex offender is not allowed on certain public properties, such as playgrounds or schools, because of prior criminal convictions. Facial recognition could be used to monitor surveillance video for potential candidates who might match the identity of the prohibited person.

Suspect or Associate Identification

Facial recognition can be used to acquire images and potentially help identify existing or new subjects of investigations or assist in exoneration of suspects.

Actual Instance - Smart Phone Digital Photo Comparison Exonerates Suspect

A witness in a gang-related assault case provided smartphone photos of the suspects to the detective working the case. One of the photos of a suspect was able to be run using facial recognition software and an investigative lead was developed. Upon further investigation confirmation of the suspect's name was made and during the investigation it was found that the suspect was in jail in another location at the time of the crime. Verification of the suspect was made based on the photo of him and the tattoos on his arm. Apparently, the witness provided an incorrect photo of one of the suspects and the facial recognition system, along with further investigation, saved investigators time, and more importantly, saved the individual from being arrested for a case in which he was not involved.[19]

[18] Safran MorphoTrust Corporation.
[19] United States National Capital Region Facial Analysis Pilot Test Project.

Actual Instance - Homicide Suspect Identified

In April of 2018, Edgewater, Colorado, Police had a shooting death resulting from an attempted random street robbery and at the onset of the investigation had no suspect information or leads. From leads that were eventually put together, police were able to identify a suspect vehicle which was impounded. A receipt to a 7-Eleven was found in the vehicle and grainy footage from the store video system was obtained showing the suspects inside the store approximately one hour after the homicide. Three of the four parties seen in the video were identified by traditional means and subsequently arrested.

A fourth suspect/witness was seen but detectives were unable to identify her. With Wheat Ridge Police help, detectives used a facial recognition program to help identify and locate this female. This person ended up being in the car at the time of the homicide and was able to tell us exactly what happened the night of the homicide, who pulled the trigger and what other roles other people inside the vehicle played.

During subsequent follow up, the suspects made incriminating statements to multiple people on Facebook about the homicide. Detectives used the facial recognition program to help identify pictures of people found on their Facebook profiles since nobody uses their real name.[20]

Actual Instance - Theft Case Solved

An investigator had a theft case where the victim met the suspect for a date. When she went to the restroom, he stole her wallet. The only thing she knew about him was his first name. She had downloaded a picture of him on her phone. The agency's facial recognition application and the statewide mug shot database, identified a high-probability candidate, returning both identity information and extensive arrest information. The detective used the application's photo lineup feature, showed it to the victim and she recognized the identified candidate immediately. Charges are pending.[21]

Actual Instance - Carjacking Suspects Found

Two men attempted a robbery of a woman in the parking lot of a liquor store. The woman bravely fought off attempts to have her wallet and car taken, and the men fled. The store owner provided surveillance video of one of the men, who had entered the store to make a small purchase while stalking the victim. The video provided an image of the suspect, which was compared to a correctional photo database, revealing potential suspect candidates. Further investigation led to the apprehension of both the man in the video and his accomplice brother.[22]

Custodial & Supervisory

The following use cases use facial recognition technologies to potentially identify and track candidates as part of efficiently operating criminal justice system programs.

[20] Edgewater, Colorado Police Department.
[21] Arapahoe County, Colorado Sheriff's Department.
[22] Greenville County, South Carolina Sheriff's Department.

Admittance Identification

Facial recognition can be used to help authenticate the identity of arrested persons being booked into detention.

Example Scenario

A person arrested by a police officer for a crime might refuse to identify themselves. The suspect is often brought to a correctional facility. Booking officers usually obtain a photo upon processing, thereby comparing it to existing photos on file to potentially positively identify the suspect.

Access Control & Movement

Identity verification of inmates or other persons can be aided via facial recognition, helping to control access to certain areas of a detention facility, or assist in confirming identity before receiving medication, privileges, or access to items restricted to other inmates.

Example Scenario

A correctional facility controls access to certain privileged areas and needs to ensure inmates required to present themselves for certain actions are properly identified. Officers can use facial recognition to corroborate with other means of identification, such as ID bracelets, RFID devices, and other biometric indicators.

Identification for Release

Confirming an inmate's identity prior to approved temporary or permanent release can be aided by facial recognition.

Example Scenario

A correctional institution obviously needs to control egress from its facility. Facial recognition can be used to help ensure an inmate presenting him or herself for work furlough, or release at the end of their sentence, is in fact the prisoner which should be allowed to leave the facility.

Identification for Program Participation

Facial recognition can be used to help confirm identity for special program participation, such as parole, probation, or sex offender registry.

Example Scenario

A parole or probation officer may be required to positively identify a person presenting himself for a urine test or mandated parole check-in visit. Facial recognition may be used to help establish a positive identity in concert with other biometric systems or identification processes.

Court Appearances

Identification of a court defendant or witness can be further corroborated using facial recognition.

Example Scenario

A judge may order a defendant appearing before her positively identified, especially in cases of identity fraud, exact twins or undocumented aliens with no official government identification. Court officers could use facial recognition to assist in the positive identity of the person by comparing the person's face with available databases.

CONCLUSION

Technologies like facial recognition systems are essential to help police maintain order in the modern world. However, their success as an effective tool for law enforcement are dependent upon ensuring that they are properly deployed and used. Additionally, law enforcement agencies must work closely with the communities to explain their use, educate the public on the capabilities, and demonstrate how the use of facial recognition technology will benefit public safety.

Recommendation #1: Fully Inform the Public

Law enforcement should endeavor to completely engage in public dialogue regarding purpose-driven facial recognition use, including how it operates, when and how images are taken and retained, and the situations in which it is used.

With facial recognition systems, the most powerful aspect is its use to compare as many images as possible in a short amount of time. It helps automate a laborious manual process to aid in many public safety efforts. Therefore, maximizing lawful and accepted use of images should be paramount, and providing the public with confidence that such capture and comparison are done fairly will ultimately ensure the most successful use of facial recognition.

[23] This idiom is widely attributed to an unknown contributing author of the National Convention Decrees during the French Revolution, May 8, 1793

[24] Sir Robert Peel, British Statesman and founder of the London Metropolitan Police in 1829.

Recommendation #2: Establish Use Parameters

Appropriate system use conditions, even preliminary ones, must be established as soon as possible to engender public confidence it its use and avoid any further proliferation of mistrust.

The use cases within this document demonstrate the varied ways in which this one technology can be deployed into many aspects of public safety. No doubt more uses will arise over time, bringing facial recognition systems to bear against all manner of crime, and on behalf of many victims, just as fingerprinting and DNA matching have done in the past.

The real cases presented are but a small sampling of the numerous success stories, many exonerating the wrongly accused as well as bringing the correct criminal to justice. It is hoped that more cases will be brought to light through enlightening discussions such as those this document attempts to create.

Recommendation #3: Publicize its Effectiveness

All public safety agencies should widely publish facial recognition success stories to heighten overall awareness of its usefulness, especially those cases in which suspects are exonerated, or where facial recognition is used to protect vulnerable persons.

This description of facial recognition systems and the ways in which it is being used by police is a starting point. While it is most often used to apprehend criminals, it is also used to find missing children, identify deceased persons and help prevent the innocent from being accused. Through consideration of the identified issues and these use cases, human reference points will be created so that the technology's interactions with citizens will be less mysterious and more appreciated for the service if provides. It is also hoped that by outlining how it is used throughout law enforcement, it will help stimulate needed conversation, policy creation and baseline training standards that can be tailored to each use within accepted community tolerances.

Recommendation #4: Create Best Practice Principles and Policies

Model law enforcement facial recognition guidance and regulation documents should be immediately established and broadly adopted, to include training benchmarks, privacy standards, human examiner requirements, and anti-bias safeguards.

Initial training and periodic re-training certifications are required as a part of most law enforcement technologies, and facial recognition seems to need such best practice standards to ensure both the courts and the public have a confidence in its consistent, fair use. Only after a broader public and judicial acceptance of facial recognition is created and stabilized can it then realize its full potential in becoming one of the most efficient and amazing law enforcement tools every deployed.

None of this catalog's representations, nor its recommendations will be constants – things change at a record pace these days, and so too must the ways in which we view and regulate ourselves as well as our machines. However, the use cases presented, and the suggestions within this report to improve the standing of facial recognition, should be immediately useful to help get this technology back on a positive trajectory.

The LEITTF believes strongly in facial recognition abilities and reasonable use conditions, and highly recommends enlisting the public more directly to generate wide support for our collective mission – to make the world a safer place.

RESOURCES

For more information about facial recognition technologies and opposition to it:

❖ IACP Technology Policy Framework	https://www.theiacp.org/sites/default/files/all/i-j/IACP%20Technology%20Policy%20Framework%20January%202014%20Final.pdf
❖ City of Palo Alto Surveillance Technology Ordinance	https://www.cityofpaloalto.org/civicax/filebank/documents/66597
❖ U.S. Bureau of Justice Assistance Policy Development Template	https://www.bja.gov/Publications/Face-Recognition-Policy-Development-Template-508-compliant.pdf
❖ Georgetown Center for Privacy & Technology Face Recognition Use Policy	https://www.perpetuallineup.org/appendix/model-police-use-policy
❖ Electronic Frontier Foundation Police Uses of Facial Recognition	https://www.eff.org/wp/law-enforcement-use-face-recognition

❖ Cardiff University Evaluation of Police Facial Recognition Use Cases	https://crimeandsecurity.org/feed/afr
❖ ACLU Report on Test Use of Facial Recognition at U.S. Capitol	https://www.aclu.org/blog/privacy-technology/surveillance-technologies/amazons-face-recognition-falsely-matched-28
❖ Michigan State University Case Study of Facial Recognition Use in Boston Bombing Investigation	http://biometrics.cse.msu.edu/Publications/Face/KlontzJain_CaseStudyUnconstrainedFacialRecognition_BostonMarathonBombimgSuspects.pdf
❖ Draft Facial Recognition Policy (James Medford, USAF Lt. Col. (Ret.)	https://drive.google.com/open?id=1BzKrSo-kLUV8uI88gwUm_1Du3ewePwVZ

REFERENCES

Georgetown University Law School Center for Privacy and Technology Report, *The Perpetual Line-Up*, October 2016, https://www.perpetuallineup.org/.

Massachusetts Institute of Technology Computer Science and Artificial Intelligence Laboratory Study, *Uncovering and Mitigating Algorithmic Bias Through Learned Latent Structure*, January 2019, http://www.aies-conference.com/wp-content/papers/main/AIES-19_paper_220.pdf.

IBM Corporation, *Diversity in Faces Study*, January 2019, https://www.ibm.com/blogs/research/2019/01/diversity-in-faces/.

ABOUT THE IJIS INSTITUTE

The IJIS Institute is a nonprofit alliance working to promote and enable technology in the public sector and expand the use of information to maximize safety, efficiency, and productivity.

The IJIS Institute has members and associates working within and across several major public-sector domains as our areas of focus:

- Criminal Justice (Law Enforcement, Corrections, Courts)
- Public Safety (Fire, EMS, Emergency Management)
- Homeland Security
- Health and Human Services
- Transportation

IJIS Institute is the only national membership organization that brings together the innovative thinking of the private sector and the practitioners, national practice associations, and academic organizations that are working to solve public sector information and technology challenges. IJIS Institute advocates for policies, processes, and information sharing standards that impact our safety and security, builds knowledge on behalf of our stakeholder groups, and connects the organizations and leaders within the communities of interest.

The IJIS Institute provides a trusted forum within and across our areas of focus where resources are developed, collaboration is encouraged, and public-sector stakeholders can realize the benefits of technology and the power of information to keep our communities safe, healthy, and thriving.

Founded in 2001 as a 501(c) (3) nonprofit corporation with a national headquarters in Ashburn, Virginia, the IJIS Institute has grown to nearly 400 member companies and individual associates from government, nonprofit, and educational institutions from across the United States.

The IJIS Institute thanks the Law Enforcement Imaging Technology Task Force for their work on this document. The IJIS Institute also thanks the many companies who have joined as Members that contribute to the work of the Institute and share in our mission to drive public-sector technology innovation and empower information sharing to promote safer and healthier communities. For more information on the IJIS Institute, visit our website at http://www.ijis.org/.

ABOUT THE INTERNATIONAL ASSOCIATION OF CHIEFS OF POLICE

The International Association of Chiefs of Police (IACP) is the world's largest and most influential professional association for police leaders. With more than 30,000 members in over 150 countries, the IACP is a recognized leader in global policing. Since 1893, the association has been speaking out on behalf of law enforcement and advancing leadership and professionalism in policing worldwide.

The IACP is known for its commitment to shaping the future of the police profession. Through timely research, programming, and unparalleled training opportunities, the IACP is preparing current and emerging police leaders—and the agencies and communities they serve—to succeed in addressing the most pressing issues, threats, and challenges of the day.

The IACP is a not-for-profit 501c(3) organization headquartered in Alexandria, Virginia. The IACP is the publisher of The Police Chief magazine, the leading periodical for law enforcement executives, and the host of the IACP Annual Conference, the largest police educational and technology exposition in the world. IACP membership is open to law enforcement professionals of all ranks, as well as non-sworn leaders across the criminal justice system. Learn more about the IACP at www.theIACP.org.

About the Law Enforcement Imaging Technology Task Force

The Law Enforcement Imaging Technology Task Force was formed in 2015 as a joint project of the IJIS Institute and the International Association of Chiefs of Police (IACP). This Task Force was created to study new imaging software, devices, and methods as a means of ensuring successful, principled, and sustainable use which is both supported by citizen and aligned with the ultimate mission – to improve public safety.

An Open Letter to Congress on Facial Recognition

September 26, 2019

Dear Member of Congress,

Facial recognition technology is one of many technologies that law enforcement can use to help keep communities safe. Facial recognition systems have improved rapidly over the past few years, and the best systems perform significantly better than humans.[1] Today facial recognition technology is being used to help identify individuals involved in crimes, find missing children, and combat sex trafficking. As the technology continues to improve, there will be even more opportunities in the future to use the technology as an investigative tool to solve crimes; as a security countermeasure against threats in airports, schools, and other public venues; and as a means to securely identify individuals at ports of entry. Indeed, travelers are already responding positively to biometric entry/exit programs that allow them to pass swiftly and securely through airports.[2]

While polls consistently show that Americans trust law enforcement to use facial recognition technology responsibly, some groups have called for lawmakers to enact bans on facial recognition technology.[3] While we agree that it is important to have effective oversight and accountability of these tools to uphold and protect civil liberties, we disagree that a ban is the best option to move forward. Bans would keep this important tool out of the hands of law enforcement officers, making it harder for them to do their jobs efficiently, stay safe, and protect our communities.

We are writing to encourage you to consider many of the viable alternatives to bans so that law enforcement can use facial recognition technology safely, accurately, and effectively. These alternatives may include expanding testing and performance standards, the development of best practices and guidance for law enforcement, and additional training for different uses of the technology.

---

[1] P. J. Phillips et al., "Face recognition accuracy of forensic examiners, superrecognizers, and face recognition algorithms," Proceedings of the National Academy of Sciences, June 12, 2018, https://www.pnas.org/content/pnas/115/24/6171.full.pdf.

[2] "Air Passengers Believe Technology Can Improve Travel," Xenophon Analytics, July 1, 2019, https://xenophonstrategies.com/technology-can-improve-travel/; "Delta expands optional facial recognition boarding to new airports, more customers," Delta, June 19, 2019, https://news.delta.com/delta-expands-optional-facial-recognition-boarding-new-airports-more-customers; "Survey: Few Americans Want Government to Limit Use of Facial Recognition Technology, Particularly for Public Safety or Airport Screening," Center for Data Innovation, January 7, 2019, https://www.datainnovation.org/2019/01/survey-few-americans-want-government-to-limit-use-of-facial-recognition-technology-particularly-for-public-safety-or-airport-screening/.

[3] "More Than Half of U.S. Adults Trust Law Enforcement to Use Facial Recognition Responsibly," Pew Research Center, September 5, 2019, https://www.pewinternet.org/2019/09/05/more-than-half-of-u-s-adults-trust-law-enforcement-to-use-facial-recognition-responsibly/.

There are many individuals from law enforcement, industry, academia, and civil society who stand ready to work with lawmakers to craft appropriate safeguards for this technology. We encourage you to continue to work with these experts to find solutions and compromises that will allow law enforcement agencies to adopt and test this important technology with appropriate oversight.

Thank you for your consideration.

Sincerely,

Organizations
Acuant, Inc.
Arm Inc.
Cognitec
Computing Technology Industry Association (CompTIA)
Consumer Technology Association
Electronic Security Association
HID Global
iBeta QA
Identification Technology Association (IdTA)
ID Technology Partners, Inc.
IJIS Institute
Information Technology and Innovation Foundation
Innovatrics s.r.o.
International Biometrics + Identity Association
Iris ID Systems Inc
JENETRIC
National Police Foundation
National Troopers Coalition
NEC Corporation of America
NetChoice
Rank One Computing Corporation
Security Industry Association (SIA)
TechNet
Thales USA
Vision-Box

Individuals
Affiliations are listed for identification *purposes only*
Maria Cardiellos, IJIS Institute
Daniel Castro, Center for Data Innovation
Warren Champ, IBIA Member
Paulo Da Silva, Cognitec Systems Pty Ltd
Dongpyo Hong, Global PD

Roger Kelesoglu, IBIA member
Joshua Kolchins, Vision Box Systems, Inc
Tovah LaDier, IBIA
James Lewis, Center for Strategic and International Studies
Doug Maccaferri, Cognitec Systems Corporation
John Mears, IBIA
Leonard Pratt, Qualcomm Technologies Inc
Ivan Quinn, Secure Planet
Diane Ragans, IJIS Institute
Cristian Tamas, TypingDNA

Question 1: Agree or disagree? The government should strictly limit the use of surveillance cameras.

Response	Overall	Age			Gender		Region			
		18-34	*35-54*	*55+*	*Male*	*Female*	*Northeast*	*South*	*Midwest*	*West*
Strongly agree	16.1%	16.6%	15.8%	15.9%	19.4%	12.9%	14.1%	18.1%	12.4%	17.9%
Somewhat agree	20.1%	19.8%	19.8%	20.8%	20.2%	20.1%	23.9%	19.3%	17.5%	21.0%
Neither agree nor disagree	34.4%	34.8%	37.2%	30.5%	31.3%	37.4%	30.5%	34.7%	38.8%	32.6%
Somewhat disagree	14.2%	14.7%	12.1%	16.3%	14.1%	14.3%	17.9%	11.7%	16.4%	13.4%
Strongly disagree	15.2%	14.1%	15.0%	16.4%	15.0%	15.3%	13.6%	16.2%	14.8%	15.0%
Total agree	36.2%	36.4%	35.6%	36.8%	39.6%	32.9%	38.0%	37.4%	29.9%	38.9%
Total disagree	29.4%	28.8%	27.1%	32.8%	29.1%	29.7%	31.5%	27.9%	31.2%	28.5%

Source: The Center for Data Innovation conducted a national online poll of 3,151 U.S. adult Internet users between December 13, 2018 and December 16, 2018. For more information, visit datainnovation.org.

Question 2: Agree or disagree? The government should strictly limit the use of surveillance cameras even if it means stores can't use them to reduce shoplifting.

Response	Overall	Age			Gender		Region			
		18-34	*35-54*	*55+*	*Male*	*Female*	*Northeast*	*South*	*Midwest*	*West*
Strongly agree	7.4%	7.4%	7.2%	7.6%	9.5%	5.4%	7.0%	9.5%	6.1%	5.5%
Somewhat agree	10.8%	13.0%	9.2%	10.4%	11.0%	10.5%	10.9%	11.4%	8.8%	11.5%
Neither agree nor disagree	23.0%	23.6%	24.1%	21.2%	20.4%	25.7%	20.9%	23.0%	25.3%	22.6%
Somewhat disagree	22.5%	21.9%	23.3%	22.2%	21.6%	23.5%	24.8%	20.5%	21.9%	24.6%
Strongly disagree	36.3%	34.1%	36.2%	38.6%	37.6%	34.9%	36.5%	35.5%	37.8%	35.8%
Total agree	18.2%	20.4%	16.4%	18.0%	20.5%	15.9%	17.9%	20.9%	14.9%	17.0%
Total disagree	58.8%	56.0%	59.5%	60.8%	59.2%	58.4%	61.3%	56.1%	59.7%	60.4%

Source: The Center for Data Innovation conducted a national online poll of 3,151 U.S. adult Internet users between December 13, 2018 and December 16, 2018. For more information, visit datainnovation.org.

Question 3: Agree or disagree? The government should strictly limit the use of surveillance cameras even if it comes at the expense of public safety.

Response	Overall	Age			Gender		Region			
		18-34	*35-54*	*55+*	*Male*	*Female*	*Northeast*	*South*	*Midwest*	*West*
Strongly agree	7.4%	9.0%	6.0%	7.5%	10.8%	4.1%	7.9%	8.2%	6.1%	7.0%
Somewhat agree	10.5%	10.8%	10.3%	10.6%	12.5%	8.6%	9.6%	11.6%	9.9%	10.1%
Neither agree nor disagree	23.5%	24.3%	25.6%	20.0%	21.6%	25.4%	19.3%	24.9%	25.8%	22.2%
Somewhat disagree	21.5%	19.5%	21.9%	23.1%	19.2%	23.8%	24.0%	18.9%	21.5%	23.7%
Strongly disagree	37.1%	36.4%	36.2%	38.9%	36.0%	38.1%	39.2%	36.3%	36.7%	37.0%
Total agree	17.9%	19.8%	16.3%	18.0%	23.3%	12.7%	17.5%	19.8%	16.0%	17.1%
Total disagree	58.6%	55.9%	58.1%	62.0%	55.2%	61.9%	63.3%	55.3%	58.2%	60.7%

Source: The Center for Data Innovation conducted a national online poll of 3,151 U.S. adult Internet users between December 13, 2018 and December 16, 2018. For more information, visit datainnovation.org.

Question 4: Agree or disagree? The government should strictly limit the use of facial recognition technology.

Response	Overall	Age			Gender		Region			
		18-34	*35-54*	*55+*	*Male*	*Female*	*Northeast*	*South*	*Midwest*	*West*
Strongly agree	12.5%	14.6%	11.7%	11.2%	15.6%	9.4%	12.4%	11.7%	10.9%	15.2%
Somewhat agree	13.7%	15.2%	14.0%	11.8%	13.8%	13.6%	12.4%	14.5%	13.9%	13.3%
Neither agree nor disagree	29.0%	31.3%	29.7%	25.5%	26.5%	31.4%	28.8%	28.3%	31.9%	27.4%
Somewhat disagree	20.5%	19.0%	20.2%	22.5%	18.8%	22.1%	21.8%	20.3%	20.0%	20.4%
Strongly disagree	24.4%	19.9%	24.4%	29.0%	25.3%	23.5%	24.7%	25.3%	23.2%	23.7%
Total agree	26.2%	29.8%	25.7%	23.0%	29.4%	23.0%	24.8%	26.2%	24.8%	28.5%
Total disagree	44.9%	38.9%	44.6%	51.5%	44.1%	45.6%	46.4%	45.6%	43.3%	44.1%

Source: The Center for Data Innovation conducted a national online poll of 3,151 U.S. adult Internet users between December 13, 2018 and December 16, 2018. For more information, visit datainnovation.org.

Question 5: Agree or disagree? The government should strictly limit the use of facial recognition technology even if it means stores can't use it to reduce shoplifting.

Response	Overall	Age			Gender		Region			
		18-34	*35-54*	*55+*	*Male*	*Female*	*Northeast*	*South*	*Midwest*	*West*
Strongly agree	12.2%	14.3%	11.4%	11.1%	14.1%	10.4%	11.7%	11.9%	10.8%	14.4%
Somewhat agree	11.6%	12.9%	11.3%	10.7%	12.6%	10.7%	11.5%	12.1%	12.0%	10.6%
Neither agree nor disagree	27.1%	29.4%	28.7%	22.6%	25.3%	28.8%	26.0%	26.6%	29.3%	26.6%
Somewhat disagree	20.9%	20.1%	19.9%	22.8%	18.9%	22.7%	24.6%	18.4%	21.8%	21.2%
Strongly disagree	28.2%	23.3%	28.6%	32.8%	29.1%	27.4%	26.1%	31.1%	26.0%	27.2%
Total agree	23.8%	27.2%	22.7%	21.8%	26.7%	21.1%	23.3%	24.0%	22.8%	25.0%
Total disagree	49.1%	43.4%	48.5%	55.6%	48.0%	50.1%	50.7%	49.5%	47.9%	48.4%

Source: The Center for Data Innovation conducted a national online poll of 3,151 U.S. adult Internet users between December 13, 2018 and December 16, 2018. For more information, visit datainnovation.org.

Question 6: Agree or disagree? The government should strictly limit the use of facial recognition technology even if it means airports can't use it to speed up security lines.

Response	Overall	Age			Gender		Region			
		18-34	*35-54*	*55+*	*Male*	*Female*	*Northeast*	*South*	*Midwest*	*West*
Strongly agree	9.6%	11.5%	9.2%	8.4%	11.8%	7.5%	8.8%	10.1%	8.5%	10.6%
Somewhat agree	10.3%	12.6%	9.4%	9.2%	11.3%	9.4%	11.7%	10.8%	9.3%	9.5%
Neither agree nor disagree	25.7%	26.7%	28.2%	21.5%	23.1%	28.3%	22.4%	25.8%	28.3%	25.6%
Somewhat disagree	20.5%	19.8%	20.3%	21.6%	19.4%	21.6%	22.2%	19.1%	21.2%	20.9%
Strongly disagree	33.8%	29.4%	33.0%	39.4%	34.4%	33.2%	34.8%	34.2%	32.7%	33.4%
Total agree	20.0%	24.1%	18.5%	17.5%	23.1%	16.9%	20.5%	20.9%	17.8%	20.1%
Total disagree	54.3%	49.2%	53.2%	61.0%	53.8%	54.9%	57.0%	53.3%	53.9%	54.3%

Source: The Center for Data Innovation conducted a national online poll of 3,151 U.S. adult Internet users between December 13, 2018 and December 16, 2018. For more information, visit datainnovation.org.

Question 7: Agree or disagree? The government should strictly limit the use of facial recognition technology even if it comes at the expense of public safety.

Response	Overall	Age			Gender		Region			
		18-34	*35-54*	*55+*	*Male*	*Female*	*Northeast*	*South*	*Midwest*	*West*
Strongly agree	8.2%	9.7%	7.9%	7.1%	10.5%	6.0%	7.4%	9.0%	6.5%	9.3%
Somewhat agree	10.1%	10.5%	10.1%	9.7%	12.2%	8.1%	9.2%	11.1%	9.6%	9.6%
Neither agree nor disagree	26.9%	27.8%	29.5%	22.6%	24.0%	29.6%	24.4%	26.7%	31.6%	24.5%
Somewhat disagree	21.1%	20.5%	20.8%	22.0%	20.0%	22.1%	25.0%	18.7%	19.9%	22.9%
Strongly disagree	33.8%	31.5%	31.7%	38.6%	33.3%	34.2%	33.9%	34.5%	32.4%	33.7%
Total agree	18.3%	20.2%	18.0%	16.8%	22.7%	14.1%	16.6%	20.1%	16.1%	18.9%
Total disagree	54.8%	52.0%	52.5%	60.6%	53.3%	56.3%	59.0%	53.2%	52.3%	56.6%

Source: The Center for Data Innovation conducted a national online poll of 3,151 U.S. adult Internet users between December 13, 2018 and December 16, 2018. For more information, visit datainnovation.org.

Question 8: Agree or disagree? Police departments should be allowed to use facial recognition technology to help find suspects if the software is correct 80% of the time.

Response	Overall	Age			Gender		Region			
		18-34	*35-54*	*55+*	*Male*	*Female*	*Northeast*	*South*	*Midwest*	*West*
Strongly agree	17.7%	17.3%	16.1%	20.0%	19.0%	16.4%	14.4%	20.3%	15.2%	18.2%
Somewhat agree	21.6%	20.8%	21.2%	23.1%	22.3%	21.0%	23.0%	21.3%	20.5%	22.2%
Neither agree nor disagree	28.5%	27.9%	30.5%	26.8%	26.1%	30.9%	26.0%	29.2%	32.0%	26.3%
Somewhat disagree	15.2%	15.4%	15.2%	15.0%	13.9%	16.5%	18.8%	13.7%	14.7%	15.6%
Strongly disagree	16.9%	18.6%	17.0%	15.0%	18.7%	15.1%	17.9%	15.5%	17.6%	17.7%
Total agree	39.3%	38.1%	37.2%	43.2%	41.3%	37.4%	37.4%	41.6%	35.7%	40.4%
Total disagree	32.1%	34.0%	32.2%	30.1%	32.6%	31.7%	36.6%	29.2%	32.3%	33.4%

Source: The Center for Data Innovation conducted a national online poll of 3,151 U.S. adult Internet users between December 13, 2018 and December 16, 2018. For more information, visit datainnovation.org.

Question 9: Agree or disagree? Police departments should be allowed to use facial recognition technology to help find suspects if the software is correct 90% of the time.

Response	Overall	Age			Gender		Region			
		18-34	*35-54*	*55+*	*Male*	*Female*	*Northeast*	*South*	*Midwest*	*West*
Strongly agree	23.4%	23.6%	20.9%	26.2%	24.6%	22.2%	21.2%	25.0%	20.6%	25.1%
Somewhat agree	23.9%	21.6%	23.9%	26.5%	22.5%	25.3%	25.1%	24.2%	21.3%	25.1%
Neither agree nor disagree	27.7%	28.6%	29.7%	24.1%	25.1%	30.2%	24.7%	28.2%	31.6%	25.3%
Somewhat disagree	11.3%	12.1%	10.4%	11.6%	12.0%	10.6%	13.6%	9.6%	11.6%	12.1%
Strongly disagree	13.7%	14.1%	15.1%	11.6%	15.7%	11.8%	15.4%	13.1%	14.9%	12.4%
Total agree	47.3%	45.2%	44.8%	52.7%	47.1%	47.5%	46.3%	49.2%	41.9%	50.2%
Total disagree	25.0%	26.2%	25.5%	23.2%	27.8%	22.3%	29.0%	22.6%	26.5%	24.5%

Source: The Center for Data Innovation conducted a national online poll of 3,151 U.S. adult Internet users between December 13, 2018 and December 16, 2018. For more information, visit datainnovation.org.

Question 10: Agree or disagree? Police departments should be allowed to use facial recognition technology to help find suspects if the software is correct 100% of the time.

Response	Overall	Age			Gender		Region			
		18-34	*35-54*	*55+*	*Male*	*Female*	*Northeast*	*South*	*Midwest*	*West*
Strongly agree	41.1%	40.9%	38.5%	44.6%	39.7%	42.6%	43.7%	41.7%	37.7%	41.5%
Somewhat agree	18.3%	18.1%	16.9%	20.2%	19.4%	17.2%	17.3%	18.2%	16.4%	20.9%
Neither agree nor disagree	24.5%	24.8%	27.3%	20.8%	23.0%	26.0%	19.9%	25.3%	28.2%	23.2%
Somewhat disagree	6.0%	6.6%	6.4%	5.1%	6.3%	5.7%	7.3%	5.8%	6.9%	4.7%
Strongly disagree	10.0%	9.7%	10.9%	9.3%	11.6%	8.5%	11.7%	9.0%	10.8%	9.7%
Total agree	59.4%	59.0%	55.4%	64.8%	59.1%	59.8%	61.0%	59.9%	54.1%	62.4%
Total disagree	16.1%	16.3%	17.2%	14.4%	17.9%	14.3%	19.0%	14.8%	17.7%	14.4%

Source: The Center for Data Innovation conducted a national online poll of 3,151 U.S. adult Internet users between December 13, 2018 and December 16, 2018. For more information, visit datainnovation.org.

Kevin Jinks

Subject Matter Expert, Department of Justice/Office of Legal Policy

Kevin Jinks is Senior Counsel in the Office of Legal Policy at the U.S. Department of Justice. He retired from the Army in 2019 after serving over 20 years as an Infantry Officer and Judge Advocate, spending his last three years as the senior legal advisor for the Army Special Mission Unit at Fort Bragg, North Carolina. After an initial year at Fort Benning, Georgia, Kevin spent three years as a platoon leader and staff officer at the 3d U.S. Infantry Regiment, The Old Guard, Fort Myer, Virginia. He spent the night of September 11, 2001, at the Pentagon attack site and then led his platoon there over the next three weeks conducting body recovery, debris removal, and security. Kevin deployed as a Judge Advocate six times to Iraq and one time to Afghanistan. He has advised at the tactical, operational, and strategic levels, including: 1st Brigade, 1st Armored Division; 5th Special Forces Group (Airborne); 101st Airborne Division (Air Assault); and the U.S. Cyber Command.

Kevin Jinks, Senior Counsel, Office of Legal Policy, Department of Justice
Reduction of Crime Technology Panel:
Opportunities and Challenges Posed by Unmanned Aircraft Systems to Public Safety and Achieving Law Enforcement and National Security Goals
April 21, 2020

INTRODUCTION

The Office of Legal Policy ("OLP") within the Department of Justice (the "Department") is honored to present this testimony about the opportunities and challenges posed by unmanned aircraft systems (UAS) to the public safety and to the accomplishment of our Nation's law enforcement and national security goals. On behalf of the Assistant Attorney General for Legal Policy, Beth Williams, I thank the President's Commission on Law Enforcement and Administration of Justice for taking up this important and timely discussion as part of its technology tools panel in the Reduction of Crime hearings. After an introductory overview of how UAS are increasingly woven into the fabric of our everyday lives, I will divide my remarks into two broad topics: first, how law enforcement and public safety agencies can responsibly employ UAS for their missions; second, some considerations regarding how federal, state, and local law enforcement can effectively address and mitigate the threat of malicious UAS. I will conclude with four concrete recommendations to this panel for how the Commission can better position the United States to achieve the many benefits offered by UAS while simultaneously protecting the public and promoting our law enforcement and national security objectives.

BRIEF OVERVIEW

UAS, more commonly referred to as "drones," are becoming ubiquitous in our society. They seem to be everywhere. The Federal Aviation Administration (FAA) projects that small model UAS use by hobbyists will grow from 1.2 million in 2018 to 1.4 million in 2023, while commercial, small non-model UAS use will triple from 277,386 in 2018 to 835,211 in 2023.[1] To facilitate the exponential growth of commercial use of UAS over the next three years, industry and the FAA are collaborating across numerous sectors, such as package and food delivery, transport of medical supplies, and delivery of over-the-counter medications.[2] The worldwide Coronavirus 2019 (COVID-19) pandemic produced even more novel uses of UAS. For example, Canadian drone company, "Draganfly," announced a partnership with the Australian Department of Defense and the University of South Australia on "pandemic drones" that use sensors and computer vision to monitor people's temperature and heart rate and detect coughing in a crowd.[3] Relatedly, the Economic Times reported last week that India has joined China in using drones to monitor public gatherings, ensure social distancing, spray disinfectants over villages, and oversee cargo in response to COVID-19.[4] Although not all such novel uses will comport with American values and legal protections for privacy and civil liberties, it is clear that personal and commercial use of UAS will continue to evolve over time, increasing the number of UAS in our skies and changing how we communicate and exchange goods and services with one another.

---

[1] Federal Aviation Administration (FAA) website, https://www.faa.gov/news/updates/?newsId=93646 (last visited April 17, 2020).
[2] FAA website, https://www.faa.gov/uas/advanced_operations/package_delivery_drone/ (last visited April 16, 2020).
[3] https://www.businessinsider.com/draganfly-pandemic-drone-will-detect-people-infected-with-coronavirus-2020-4 (last visited, April 19, 2020).
[4] Economic Times website, https://economictimes.indiatimes.com/news/politics-and-nation/covid-19-lockdown-authorities-rely-on-drone-eye-to-maintain-vigil/articleshow/75112745.cms (last visited April 19, 2020).

BEST PRACTICES FOR LAW ENFORCEMENT AND PUBLIC SAFETY USE OF UAS

Just as personal and commercial use of UAS continues to expand and evolve, law enforcement and public safety use of UAS likewise continues to expand and evolve. Law enforcement agencies across the country have recognized that UAS save officers' lives and so have built UAS programs and are working to identify effective uses of UAS technology as well as appropriate policies and safeguards to protect privacy and civil liberties. This is no different at the Department of Justice, which uses UAS to support crime scene response and investigation, search and rescue, and site security, among other authorized uses, and we continue to grow our programs. Over the past year, for example, the Federal Bureau of Investigation (FBI) has transitioned from using UAS as a niche headquarters capability to deploying at least two UAS in every FBI field office in the country for use in a variety of circumstances. Additional examples of law enforcement and public safety use of UAS include: providing situational awareness of areas that cannot be seen from the ground; providing up-close, real-time view of a crime scene allowing officers to remain at a safe distance without exposing themselves to unknown and unseen risks; bomb and hazardous materials observation; traffic collision reconstruction and crime scene documentation; disaster response; and clearing the top of a building on approach during fugitive apprehension.

With increased opportunity offered by constantly improving technology that allows UAS to fly faster, see farther, and carry and do more, comes great challenge and responsibility. UAS are a tool that Federal and State, local, tribal, and territorial (SLTT) law enforcement and public safety agencies should responsibly embrace and increasingly incorporate into their operations to better protect the public and enforce the law. There are a number of helpful publications that provide recommendations and detail numerous best practices that should be considered by any law enforcement agency considering a UAS program; two specific ones I will mention are 1) the Department's report entitled, "Drones: A Report on the Use of Drones by Public Safety Agencies – and a Wake-up Call about the Threat of Malicious Drone Attacks,"[5] published this week by the Department's Community Oriented Policing Services Office, or "COPS Office," and 2) "Considerations and Recommendations for Implementing an Unmanned Aircraft Systems (UAS) Program," published in December 2016 by the Department's National Institute of Justice.[6] While time does not permit discussing all of those best practices, I want to highlight five of them here. In doing so, the best practices I will discuss are on display in the Department's own Policy on the Use of Unmanned Aircraft Systems[7] (the "DOJ UAS Policy"), which the Attorney General issued in 2019 and can serve as a model for SLTT in responsibly leveraging UAS.

First, law enforcement agencies must take steps to ensure that their use of UAS includes appropriate safeguards and protections for privacy and civil liberties. As with any law

---

[5] Community Oriented Policing Services (COPS) website, COPS Office Resource Center, https://cops.usdoj.gov/RIC/ric.php?page=detail&id=COPS-W0894 (last visited April 20, 2020).
[6] Office of Justice Programs website, National Criminal Justice Reference Service, https://www.ncjrs.gov/pdffiles1/nij/250283.pdf (last visited April 19, 2020).
[7] Department of Justice (DOJ) website, Justice Manual, Title 9: Criminal, Chapter 9-95.000, https://www.justice.gov/jm/9-95000-unmanned-aircraft-systems-uas#9-95.100 (last visited April 20, 2020).

enforcement tool, it is important that the promise of new technology does not compel us to forget about the values and rights that we as public servants are sworn to protect. Policies governing the use of UAS can help. For example, the DOJ UAS Policy mandates annual privacy reviews of UAS programs and assessments of any new UAS technology from a privacy perspective. The DOJ UAS Policy places limits on data retention, generally requiring privacy sensitive data to be deleted within 180 days unless certain exceptions are met. Department UAS may only be used in connection with properly authorized investigations and activities, which prevents misuse and the misperception that they will be used for loosely defined and potentially illegal surveillance purposes.

Second, successful SLTT UAS programs have demonstrated that communication and continual engagement with the local population is key. Successful SLTT UAS programs engage the public in multiple forums; establish transparency and maintain open communications; seek out views of interested stakeholders before operationalizing UAS programs; and plan meetings at different times of the day, demonstrate the equipment, and explain potential uses (*e.g.*, helping to find an elderly person with dementia, like the Fairfax County, VA, Police Department). All of these methods have helped SLTT plan, equip, and implement UAS programs that adequately inform and involve the public and address concerns about degradation of privacy and civil liberties and infringement of Constitutional rights.

Third, law enforcement agencies should be thoughtful and deliberate about the training required to operate UAS. Effective UAS programs have policies that set training standards; incorporate practical, hands-on instruction (*e.g.*, check rides prior to operational use); ensure that training requirements address both operational training as well as policy and law (*i.e.*, policies do no good if people do not know and use them); reevaluate policy and program elements over time; and ensure that the requirements extend to operators, trainers, and supervisors alike so that there is effective leader program management and oversight. The DOJ UAS Policy and many SLTT policies are models in all of those respects.

Fourth, law enforcement agencies must be attuned to the cybersecurity and supply chain risks associated with UAS. The DOJ UAS Policy requires components to evaluate UAS acquisitions for cybersecurity risks, guarding against potential threats to the supply chain and to the Department's networks. The Department's Office of the Chief Information Officer works with component information security specialists and shares information about threats and vulnerabilities freely with the interagency and with SLTT partners. More now than ever, SLTT jurisdictions must consider these risks on the front end and appropriately mitigate them. This is not solely about the risk that a foreign entity might gain unauthorized access to law enforcement and public safety agency data from drones—although that is certainly a risk that should not be underestimated or unappreciated. This is also about mitigating risks to prevent the bad guys, *i.e.*, the targets of investigations and the hackers who would seek to keep their activities shielded, from exploiting those same vulnerabilities and gaining access to IT systems. Additionally, any responsible assessment of cybersecurity and supply chain risks will include a recognition that legislatures and executives at the federal and state level are moving to limit public agencies' purchase and deployment of certain foreign-made UAS, in light of the risks they present. That

recognition should likely result in strong consideration of procurement of UAS made domestically or by trusted allies, though each purchase decision will depend on the specific use case, mission requirements, and assessed risks.

Finally, I want to highlight for the Commission that SLTT law enforcement and public safety agencies must invest in relationships with the FAA. The Department's COPS office facilitates biannual meetings of an SLTT UAS Working Group to compile best practices and exchange ideas between SLTT law enforcement and public safety agencies; it comes as no surprise that the FAA holds a seat on that group. It is through investment in that relationship and through participation in pilot program opportunities that jurisdictions like the Chula Vista Police Department, an FAA Integration Pilot Program (IPP) member,[8] are able to employ UAS, *e.g.*, in a "Drones as First Responders" (DFR) program.[9] Using UAS to respond to emergency calls streaming high-definition video back to a department operations center, Chula Vista is able to be "present" at the scene in moments, flying beyond visual line of sight up to three miles, and gain situational awareness of what is happening before officers arrive and may be placed in harm's way. Organizations must invest in an FAA relationship.

MEASURES TO PROTECT AGAINST THE THREAT OF MALICIOUS UAS

Now, I want to turn to discussing the need to protect the public from the threat of unlawful and malicious UAS. There are three specific considerations I want to address: (1) the laws available to us to investigate and prosecute the malicious and harassing use of UAS; (2) the authority to use technology that can mitigate a threatening UAS; and (3) the need for law enforcement agencies to engage with the FAA as it further develops the regulatory framework under which private, government, and commercial UAS will operate in our skies.

After careful study and discussion with interagency partners, the Department has determined that the criminal enforcement tools available to the government are fragmentary, inadequate, and insufficient to deter unlawful and malicious use of UAS. For example, the use of a weaponized drone in a fatal attack would violate Public Law 115-254 § 363, with a $25,000 civil penalty being the maximum sanction. Drone intrusions by terrorists and spies upon national defense airspace to surveille potential targets or obtain intelligence are merely misdemeanors under 49 U.S.C. § 46307. This means we may lack adequate authorities for cases against bad actors who truly intended to do harm, and it also means there is little to deter the throngs of "clueless and careless" UAS operators who fly into protected airspace, which can interfere with critical public safety operations and make it difficult for us to identify real threats. Enacting a comprehensive criminal provision, with adequate penalties and grounds of federal jurisdiction, can address the most serious and dangerous misuses of UAS. The Department is currently developing a recommendation for legislation to do just that.

---

[8] FAA website, https://www.faa.gov/uas/programs_partnerships/integration_pilot_program/ (last visited April 19, 2020)(the FAA's Integration Pilot Program unites state, local, and tribal governments together with private sector entities to explore new uses of UAS in the National Airspace System, with one major benefit being accelerated approval of new UAS operations requiring special FAA approval).

[9] Chula Vista Police Department website, https://www.chulavistaca.gov/departments/police-department/programs/uas-drone-program (last visited April 16, 2020).

Relatedly, the laws and regulations on the books are only as good as they are applied. Both on the criminal and the FAA civil enforcement side, we must apply the laws and regulations to hold UAS operators accountable for misuse. In partnership with the FAA, the Department has begun to do that in the events where we have partnered with SLTT jurisdictions to protect special events by issuing summons, making arrests, prosecuting based on current authorities, such as failure to register a drone, and assessing civil fines. Together, a comprehensive drone enforcement criminal statute that augments our prosecution authorities, coupled with increased enforcement, will help create a culture of compliance.

Turning to the legal authority to mitigate UAS, Congress authorized the Attorney General and the Secretary of the Department of Homeland Security (DHS) in the 2018 Preventing Emerging Threats Act ("the Act"), codified at 6 U.S.C. § 124n, to protect people and places from the credible threat posed by UAS by taking certain actions notwithstanding other federal laws that might make those actions illegal (for example, jamming or taking control of a threatening drone). The Attorney General issued the Department's C-UAS Guidance[10] implementing the Act just last week, and said it best in the Department's press release: the C-UAS Guidance will "ensure that we are positioned for the future to address this new threat, and that we approach our counter-drone efforts responsibly, with full respect for the Constitution, privacy, and the safety of the national airspace."[11] To date, under interim guidance, the Attorney General has authorized C-UAS protection activities at eight major special events since February 2019, including Super Bowl LIII in Atlanta in 2019, the 2019 World Series in both Washington, D.C., and Houston, Texas, and Super Bowl LIV in Miami in 2020.

Many of the SLTT jurisdictions we worked with at those events, and throughout the country, want the legal authority that DOJ has. The Department gained critical insight and important lessons-learned through those eight events. For example, we learned that you can identify and very quickly mitigate the vast majority of the UAS by having good detection technology that does not violate federal law, coupled with a ground game to quickly locate the operator and have the operator bring down the UAS. Additionally, we learned that at some events it will be important to have technology available that disrupts control of the UAS, seizes control of the UAS through technical means, or otherwise prevents the UAS from approaching a protected area. Importantly, we recognize that the federal government, in the Department and DHS, cannot be everything to everyone, everywhere, and we cannot be at every special event throughout the country that warrants UAS mitigation. The Department recommends that the Administration and Congress chart a path towards incrementally providing SLTT greater authority to mitigate UAS threats under appropriate circumstances without having to always rely on DOJ and DHS.

Finally, law enforcement agencies should care about how the FAA and other agencies are setting up regulatory framework and airspace for expanded UAS use through things like UAS Traffic Management and Remote Identification ("Remote ID"). How the FAA treats these issues

---

[10] DOJ website, available at https://www.justice.gov/ag/page/file/1268401/download (last visited April 20, 2020).
[11] DOJ website, available at https://www.justice.gov/opa/pr/attorney-general-barr-issues-guidance-protect-facilities-unmanned-aircraft-and-unmanned (last visited April 19, 2020).

will have a large impact on law enforcement, including at the local level. There is an opportunity, while these regulations are being developed, for law enforcement agencies to productively engage with the FAA on important questions such as (a) which entities will have control over and access to U.S. airspace for UAS; (b) how can law enforcement agencies safely integrate their UAS operations into the airspace, including when there is a need for operational security (secrecy); (c) who will have access to drone traffic data; and (d) is drone traffic data available for law enforcement investigation and use. Our experience in partnering with the FAA has demonstrated that they are responsive when we identify specific needs for law enforcement and public safety that can be addressed in the regulatory frameworks they are building.

NEXT STEPS - SPECIFIC RECOMMENDATIONS TO THE COMMISSION

The Commission can take the following actions to support the Department and SLTT in accomplishing our law enforcement and national security objectives and better protect the public:

1. Recommend continued responsible use of UAS by law enforcement and public safety agencies throughout the country using the 2019 DOJ UAS Policy and best practices from SLTT jurisdictions collected and published by the Department's COPS Office and National Institute of Justice.

2. Recommend Administration support for, and Congressional passage of, a comprehensive drone enforcement criminal statute that addresses the gaps in current authorities to better deter and punish the malicious and unlawful use of UAS.

3. Recommend the Administration and Congress chart a path towards incrementally providing SLTT law enforcement and public safety agencies greater authority to mitigate UAS threats under appropriate circumstances.

4. Recommend law enforcement agencies collaborate with the Department of Transportation and the FAA to identify the specific needs of law enforcement and public safety agencies and incorporate those needs into the regulatory framework around the UAS Traffic Management ecosystem and its components, such as Remote ID.

Thank you for the opportunity to share my testimony with the Commission and for considering these recommendations.