January
2017
Volume 65
Number 1

United States
Department of Justice
Executive Office for
United States Attorneys
Washington, DC
20530

Monty Wilkinson
Director

Contributors' opinions and statements should not be considered an endorsement by EOUSA for any policy, program, or service

The United States Attorneys' Bulletin is published pursuant to
28 C F R § 0 22(b)

The United States Attorneys' Bulletin is published bimonthly by the Executive Office for United States Attorneys, Office of Legal Education,
1620 Pendleton Street,
Columbia, South Carolina 29201

Editor
K Tate Chambers

Assistant Editor
Becky Catoe-Aikey

Law Clerks
Sarah Tate Chambers
Joseph Giordano
Emily Godwin

Internet Address
https://www justice gov/usao/resources
/united-states-attorneys-bulletins

Send article submissions
to Editor,
United States Attorneys' Bulletin,
National Advocacy Center,
Office of Legal Education,
1620 Pendleton Street,
Columbia, SC 29201

Cite as:
65 U S Attorneys' Bulletin, Jan 2017

Forensic Science and Forensic Evidence I

In This Issue

Introduction

Sally Q. Yates
Acting Attorney General

Forensic science plays a crucial role in our criminal justice system. Using the tiniest shreds of evidence, whether a drop of blood or a shell casing found at the scene, forensic scientists can help investigators learn who committed a crime and how it was committed. Judges and juries put great stock in this type of forensic testimony, and when presented at trial, such evidence can make the difference between conviction and acquittal.

But it is precisely because forensic evidence can be so powerful and so persuasive that we must be careful in how it is used. Even in the most advanced forensic disciplines, there are limits on what the science can reveal. In recent years, for example, we have seen the risks that forensic science presents, as we learned that certain experts have overstated the strength of the evidence in their lab reports and at trial. These errors have not simply called into question the validity of individual prosecutions, but also threatened to undermine the public's confidence in forensic science more broadly.

To address this, the Department of Justice has taken a number of steps to strengthen forensic science. In 2013, the Department partnered with the National Institute of Standards and Technology to establish the National Commission on Forensic Science (NCFS), a federal advisory committee that makes forward-looking policy recommendations to the Attorney General on forensic science topics. As Deputy Attorney General, I have had the privilege of serving as the Co-Chair of NCFS, which has developed a number of significant proposals on the practice of forensic science in both the laboratory and the courtroom. In addition, in early 2016, the Department recruited Dr. Victor Weedn to help develop new policies and guidance across DOJ's investigative agencies, research offices, and litigating components. Dr. Weedn, who serves as the chairman of the department of forensic science at George Washington University and recently completed a term as the president of the American Academy of Forensic Sciences, has spearheaded a number of important initiatives during his time at Main Justice and helped coordinate this issue of *USA Bulletin*.

One of the Department's most significant ongoing projects in this area is the multi-year development of the "Uniform Language for Testimony and Reports," or ULTRs. Once finalized, the ULTRs will outline the specific statements that the Department's forensic experts may – and may not – make when testifying in court about their scientific conclusions, thus limiting the risk of experts overstating the accuracy or reliability of a particular forensic technique. We expect that the guidance contained in the ULTRs will also prove useful for prosecutors, who will be able to rely on the documents to ensure that they properly characterize their forensic evidence in *Daubert* hearings, witness

examinations, and jury summations. The Department's Office of Legal Policy, along with experts at FBI, ATF, and DEA, remains hard at work on the project. Draft versions of the ULTRs were posted for public comment in mid-2016, and final versions are likely to be published later this year.

As you read through this issue of the *USA Bulletin*, you'll see the many ways forensic science impacts federal prosecutions, from investigations on the internet to theft of historical artifacts. I hope you find the material informative and that it provides an opportunity to learn more about the important work underway across the Department to strengthen the practice of forensic science.

Recent Developments in the Forensic Sciences

Dr. Victor W. Weedn
Senior Forensic Advisor to the Deputy Attorney General
Office of the Deputy Attorney General

I. Introduction

Forensic science is generally dated to Hans Gross' *Handbuch für Untersuchungsrichter, Polizeibeamte, Gendarmen* (*Handbook for Magistrates, police officials, military policemen*), which was published in 1893, although forensic medicine and forensic toxicology are much older. Edmond Locard established the first crime laboratory in 1910 in Lyon, France. Depending on who is to be believed, the first crime laboratory in the United States was established in Los Angeles or Berkeley, California, in 1923. The FBI laboratory was established in 1932. Throughout the first half of the twentieth century, forensic science laboratories were established throughout the United States. Although the International Association for Identification has origins dating back to 1915, most professional forensic science associations were established during the second half of the century. Initial efforts towards standardization in the field soon followed. Perhaps more importantly, gas chromatography-mass spectrometers (GC-MS) were not in widespread use until the 1970s, and genetic analyzers were not in widespread use until the 1990s. Both are the basic laboratory instruments of modern crime labs. The television show *CSI* captured the attention of the public when it first aired in 2000. Particularly with the rise of databases (fingerprints, DNA, firearms), forensic science laboratories became increasingly powerful and increasingly important to the criminal justice system. The criminal justice system has had to adapt to this new reality; for instance, in addition to appeals based upon unfair process, actual innocence became a basis for appeals in DNA prosecutions. In this article, I will discuss some major developments in forensic science policy over the past several years.

II. 2009 National Academies of Sciences (NAS) Report

In February of 2009, shortly after President Obama took office, the National Research Council (NRC) of the National Academies of Science (NAS), supported by National Institute of Justice (NIJ) funding, published its influential report, *Strengthening Forensic Science in the United States: A Path Forward*. NAT'L ACAD. OF SCI., NAT'L RESEARCH COUNCIL, STRENGTHENING FORENSIC SCIENCE IN THE UNITED STATES: A PATH FORWARD (2009). The 2009 NAS Report on forensic science was not the first call for forensic science reform in America, but one that captured the attention of policymakers. Judge Harry T. Edwards and statistician Constantine Gatsonis, co-Chairs, speaking for their committee, concluded:

> The forensic science system, encompassing both research and practice, has serious problems that can only be addressed by a national commitment to overhaul the current structure that supports the forensic science community in this country. This can only be done with effective leadership at the highest levels of both federal and state governments, pursuant to national standards, and with a significant infusion of federal funds.

Id. at *xx*

The NAS Report made 13 recommendations (paraphrased here):

1. Create a National Institute of Forensic Sciences (NIFS);
2. Standardize terminology and reporting practices;
3. Expand research on the accuracy, reliability, and validity of the forensic sciences;
4. Remove forensic science services from the administrative control of law enforcement agencies and prosecutors' offices;
5. Support forensic science research on human observer bias and sources of error;
6. Develop tools for advancing measurement, validation, reliability, information sharing, and proficiency testing, and to establish protocols for examinations, methods, and practices;
7. Require the mandatory accreditation of all forensic laboratories and certification for all forensic science practitioners;
8. Laboratories should establish routine quality assurance procedures;
9. Establish a national code of ethics with a mechanism for enforcement;
10. Support higher education in the form of forensic science graduate programs, to include scholarships and fellowships;
11. Improve the medico-legal death investigation system;
12. Support Automated Fingerprint Identification System interoperability through developing standards; and
13. Support the use of forensic science in homeland security

The NAS Report has been referred to by many courts and was quoted by Justice Scalia in *Melendez-Diaz v. Massachusetts*, 557 U.S. 305 (2009) "to refute the suggestion that this category of evidence is uniquely reliable," but Justice Kennedy in his dissent writes:

> State legislatures, and not the Members of this Court, have the authority to shape the rules of evidence. The Court therefore errs when it relies in such great measure on the recent report of the National Academy of Sciences. *Ante*, at 12–14 (discussing National Research Council of the National Academies, Strengthening Forensic Science in the United States: A Path Forward (Prepublication Copy Feb. 2009)). That report is not directed to this Court, but rather to the elected representatives in Congress and the state legislatures, who, unlike Members of this Court, have the power and competence to

determine whether scientific tests are unreliable and, if so, whether testimony is the proper solution to the problem. *Id*. at p. 23.

Several bills have been introduced into Congress without passage; it is the Executive Branch that has most vigorously responded to the NAS Report.

III. Subcommittee on Forensic Science (SoFS)

In July 2009, the White House's Office of Science and Technology Policy (OSTP) created a "Subcommittee on Forensic Science" (SoFS) to address the issues raised by the NAS report. The SoFS oversaw five interagency working groups (Accreditation and Certification; Standards, Practices, and Protocols; Education, Ethics, and Terminology; Research, Development, Testing, and Evaluation; and Outreach and Communication), which were responsible for most of the work. SoFS participation spanned 23 federal departments and agencies, and was comprised of nearly 200 federal subject matter experts and 49 individuals representing state and local forensic scientists. This body completed its work December 2012 and published its report, *Strengthening the Forensic Sciences*, in May 2014. NAT'L SCI. & TECH. COUNCIL'S SUBCOMM. ON FORENSIC SCI., STRENGTHENING THE FORENSIC SCIENCES (2014). The report recommended, among other things, the accreditation of forensic science service providers, the certification of forensic examiners and medicolegal personnel, proficiency testing for forensic examiners, and a national code of ethics for forensic service providers.

IV. National Commission on Forensic Science (NCFS)

In 2013, DOJ partnered with the National Institute of Standards and Technology (NIST) to establish the National Commission on Forensic Science (NCFS) as part of the Department's efforts to strengthen and enhance the practice of forensic science.

The Commission is co-chaired by the Deputy Attorney General and the Director of NIST, and consists of 29 voting commissioners and eight *ex officio* non-voting commissioners. The Commission includes federal, state, and local forensic science service providers; research scientists and academics; law enforcement officials; prosecutors, defense attorneys and judges; and other stakeholders from across the country. The work of the commission is supported by several subcommittees: Interim Solutions, Accreditation and Proficiency Testing; Human Factors; Medicolegal Death Investigation; Reporting and Testimony; and Scientific Inquiry and Research.

As a federal advisory committee, NCFS develops recommendations for consideration by the Attorney General. These recommendations are drafted by the subcommittees and then sent to the full body for a vote by all Commissioners. If approved, a copy of the recommendation is delivered to the Attorney General, who typically responds within six months. To date, the Attorney General has agreed to adopt several NCFS's recommendations, either in whole or in part, as discussed in greater depth elsewhere in this issue of the Bulletin. For more information, visit https://www.justice.gov/ncfs.

V. NIST Organization of Scientific Area Committees (OSAC)

Also in 2013, DOJ partnered with NIST to create the Organization of Scientific Area Committees (OSAC), which assists development of scientific standards in the various forensic science disciplines. The definitions, protocols, and practices, which comprise the "documentary standards" and guidelines considered by the OSAC, are actually promulgated by various Standards Development Organizations (i.e. ASTM, ASB, NFPA, etc.), but only "approved" standards and guidelines are posted to a National Registry.

The OSAC is composed of five scientific area committees (Biology/DNA, Chemistry/Instrumental Analysis, Crime Scene/Death Investigation, Digital/Multimedia, Physics/Pattern Interpretation) that oversee 25 subcommittees (covering the topic areas of the previous SWGs). The five SACs are overseen by the Forensic Science Standards Board (FSSB). The Human Factors, Quality Infrastructure, and Legal Resource committees also answer to the FSSB.

At the time of this writing, three standards have been posted to the National Registry of OSAC Approved Standards, but many others are in the pipeline. For more information, visit: https://www.nist.gov/forensics/organization-scientific-area-committees-forensic-science.

VI. Microscopic Hair Comparison Analysis (MHCA) Review

In response to a series of exonerations, beginning in late 2012, the DOJ and the FBI, with the collaboration of the Innocence Project (IP) and the National Association of Criminal Defense Lawyers (NACDL), reviewed laboratory reports and scientific testimony provided by FBI laboratory examiners in microscopic hair comparison analysis (MHCA) cases to identify statements that exceed the limits of science.

The review involved over 21,550 closed MHCA cases conducted prior to the year 2000. Of those cases, 3,189 involved a probative association between an evidentiary hair and a known hair sample. Many of these cases involved trials where a transcript of examiner testimony was available for review, although some resulted in guilty pleas prior to trial where only the original lab report was available for review. The majority of the FBI examiner testimony was provided in state court prosecutions.

The FBI, IP, and NACDL agreed to the basis of the MHCA review—namely, that individual statements in reports or testimony that, when viewed alone, did not meet accepted scientific standards, with no assessment of materiality regarding the impact of the report or testimony on the proceeding. The larger context of the complete testimony was not considered, including other language elsewhere that may have mitigated or corrected the overstatement. Language that had more than one interpretation was often conservatively marked as an error.

As part of this process, reviewers categorized potential errors into one of three "types":

- **Error Type 1:** The examiner stated or implied that the evidentiary hair could be associated with a specific individual to the exclusion of all others.
- **Error Type 2:** The examiner assigned to the positive association a statistical weight or probability, or provided a likelihood that the questioned hair originated from a particular source, or rendered an opinion on the likelihood or rareness of the positive association that

could lead the jury to believe that valid statistical weight can be assigned to a microscopic hair association.

- **Error Type 3:** The examiner cited the number of cases or hair analyses worked in the lab and the number of samples from different individuals that could not be distinguished from one another as a predictive value to bolster the conclusion that a hair belongs to a specific individual.

An identified error does not necessarily mean that a conviction is invalid or even that the hair analysis evidence contributed to the conviction. DOJ notifies any identified statement errors to prosecutors and defense counsel so they may assess the materiality of the statements. If it is determined by the prosecutor's office that additional testing is necessary, or if a court orders such testing, the FBI provides DNA testing if the relevant evidence is in the government's possession or control.

In April 2015, FBI, IP, and NACDL issued a joint press release in which the FBI acknowledged that at least 90 percent of trial transcripts analyzed as part of the MHCA review contained erroneous statements. Press Release, Fed. Bureau of Investigation, FBI Testimony on Microscopic Hair Analysis Contained Errors in at Least 90 Percent of Cases in Ongoing Review (April 20, 2015). The FBI found that 26 of 28 FBI agent/analysts provided either testimony with erroneous statements or submitted laboratory reports with erroneous statements. The review found that the overstated forensic matches favored prosecutors in over 95 percent of the trials reviewed.

The FBI has not completed their review as of the time of this writing, but it is nearing completion. The Texas Forensic Science Commission has also reviewed Texas state cases involving MHCA, although that review found a smaller percentage of cases with erroneous statements. Several other states are also conducting or preparing to conduct their own MCHA reviews in the future.

VII. Uniform Language for Testimony and Reports (ULTRs)

At the 10th meeting of the NCFS in June 2016, the Department announced that it was developing guidance documents governing the testimony and reports of its forensic experts. This guidance, known as the "Uniform Language for Testimony and Reports" (ULTR), clarifies what scientific statements DOJ's forensic experts may— and may not—use when testifying in court and drafting reports. The FBI currently uses Approved Scientific Standards for Testimony and Reports (ASSTRs) for this purpose.

The Department released draft versions of these guidance documents for public comment in mid-2016. Press Release, Dept. of Justice, Justice Department Issues Draft Guidance Regarding Expert Testimony and Lab Reports in Forensic Science (June 3, 2016). The draft documents were posted in two batches and cover fifteen forensic science disciplines: anthropology, body fluid testing (serology), explosive chemistry, explosive devices, fibers, footwear/tire treads, general chemical analysis, geology, glass, hair, latent fingerprint, metallurgy, mitochondrial DNA, paints/polymers, and toxicology. The Department received hundreds of comments and continues to review and revise the draft ULTRs. Once finalized and adopted, the ULTR documents will apply to all Department personnel, including forensic experts at FBI, ATF, and DEA. The exact timing for the release of the final ULTRs is unknown, although the Department hopes to complete its work in 2017.

Information on the FSDRs may be found on the DOJ forensics website at: https://www.justice.gov/forensics.

VIII. Forensic Science Discipline Reviews (FSDRs)

At the February 2016 meeting of the American Academy of Forensic Science (AAFS), Deputy Attorney General Yates announced that DOJ would review other forensic science disciplines, beyond microscopic hair comparison analysis. She suggested a quality assurance-like review for testimonial overstatements, not triggered by any specific cases or known or suspected problems, but as responsible oversight.

The Department elicited significant input through presentation of the framework, and then a more detailed plan for the Forensic Science Discipline Reviews (FSDR) was presented to the NCFS and posted for public comment, and a Statistician Roundtable was held. After deliberation, the goal of the FSDRs was declared to be "to advance the use of forensic science in the courtroom by understanding its use in recent cases and to facilitate any necessary steps to ensure that expert forensic testimony is consistent with scientific principles and just outcomes." DEP'T OF JUSTICE, FORENSIC SCI. DISCIPLINE REVIEW OF TESTIMONY (2016). The FSDR will compare testimony in a case against the underlying report to ensure that statements conformed with the report. Once the review begins, identified instances of non-conformity will trigger further review and notification of the prosecution and defense.

Information on the FSDRs may be found on the DOJ forensics website at: https://www.justice.gov/forensics.

IX. President's Council of Advisors on Science and Technology (PCAST) Report on Forensic Science

In September 2016, The President's Council of Advisors on Science and Technology (PCAST) issued a report titled *Forensic Science in Criminal Courts: Ensuring Scientific Validity of Feature-Comparison Methods*. EXEC. OFFICE OF THE PRESIDENT, PRESIDENT'S COUNCIL OF ADVISORS ON SCI. & TECH., FORENSIC SCIENCE IN CRIMINAL COURTS: ENSURING SCIENTIFIC VALIDITY OF FEATURE-COMPARISON METHODS (2016). The report took the position that unless a forensic discipline has been "scientifically validated"—in other words, unless a discipline has a known error rate—then judges should not allow the admission of expert testimony in that discipline. The report examined several specific forensic disciplines and concluded that several, including firearms, shoeprints, complex-source DNA, and bite marks, were not sufficiently validated and, therefore, expert testimony about these disciplines should not be admitted at trial.

Shortly after the report's release, Attorney General Loretta Lynch issued a statement indicating that the Department disagreed with certain findings and that it would not be adopting the report's recommendations related to the admissibility of forensic science evidence. Gary Fields, *White House Advisory Council Report Is Critical of Forensics Used in Criminal Trials*, WALL ST. JOURNAL (Sept. 20, 2016). Since then, in a handful of cases, defense attorneys have filed *in limine* motions seeking to exclude the admission of expert forensic testimony. To date, these efforts have been unsuccessful. U.S. v. Chester (U.S. Dist Ct, N Dist Ill., Eastern Div; No. 13 CR 00774, Oct. 7, 2016), IL v. Thompson (Cook Cnty Cir Ct, 13 CR 426, Oct 25, 2016), MA v. Legore (Suffolk Cnty Superior Ct; SUCR 2015-10363, Nov 17, 2016), MN v. Yellow (6th Dist Ct; No. 69DU-CR-15-1363, Oct 28, 2016).

X. Forensic Science Research and Development

While all the above has transpired, the forensic science community around the world has continued research and development efforts and made substantial progress. During this administration, technologies introduced in the forensic science community include High Resolution and Q-TOF mass spectrometers, Rapid DNA Identification instruments, Next Generation Sequencers, and 3D laser-doppler crime scene scanners. NIJ alone funds more than $100M of forensic science and DNA-focused programming in forensic science research, forensic science practice improvement, and reduction of backlogs of untested sexual assault kits. In 2015, NIJ distributed $27.5M for research, development, testing, and evaluation; $69.8M for support of publicly-funded laboratories, police departments, and law enforcement agencies; and $6.6M for training and technical assistance. NAT'L. INST. OF JUSTICE, PROJECTS FUNDED UNDER FISCAL YEAR 2015 SOLICITATIONS (2015).

The OSTP recently formed a Forensic Science Research and Development Task Force.

XI. Medicolegal Death Investigation

The NCFS has had a Medicolegal Death Investigation (MDI) Subcommittee that submitted several work products approved by the Commission in the area of medicolegal death investigation. The Department contacted the White House OSTP to form a MDI Working Group.

XII. Conclusion

Substantial shifts in forensic science policy have occurred in recent years and will continue to occur for the foreseeable future. Perhaps, these can be summed up as greater attention and scrutiny, as well as a growing national shaping of the standards in the field.

ABOUT THE AUTHOR

❑ **Dr. Victor W. Weedn** is the Senior Forensic Advisor to the Deputy Attorney General, on detail from his position as Professor and Chair of the George Washington University Department of Forensic Sciences. He is a graduate of the Southwestern Medical School and the South Texas College of Law. He underwent anatomical and clinical pathology residency training at the Baylor College of Medicine and the University of Texas Health Science Center at Houston, and then anatomic pathology fellowship training at the M.D. Anderson Hospital and Tumor Institute, and forensic pathology fellowship training at the Armed Forces Institute of Pathology. He established the Armed Forces DNA Identification Laboratory and was involved in pioneering efforts to establish STR and mitochondrial DNA sequencing methods. He directed the effort to create the current inspection and accreditation program of the National Association of Medical Examiners. Subsequently, he has had several positions, including as a medical examiner, a crime laboratory director, research scientist, and professor. He is the immediate Past President of the American Academy of Forensic Sciences.

Mobile Device Forensics: Beyond Call Logs and Text Messages

Daniel Ogden
Senior Digital Investigative Analyst
Cybercrime Lab
Computer Crime & Intellectual Property Section

I. Introduction

Throughout the year 2016, the Computer Crimes and Intellectual Property Section (CCIPS) Cybercrime Lab saw an increase in the number of supports and inquires relating to mobile devices. These inquiries include questions about how data is stored, whether the data is recoverable, and whether you can get the data if the device is locked.

As we all know, the mobile device market, which includes cellphones and smartphones, is rapidly growing. The market growth has allowed manufacturers to create thousands of different phone models we see in use today. These different models have brought many challenges to examiners when tasked with extracting and analyzing data from mobile devices. The technology involved with mobile devices is also advancing, which allows manufacturers to release new models of phones each year, with thinner cases, better graphics, faster processors, more storage, and yes, better security features.

Since the release of the first smartphones, Apple's original iPhone (running iPhone OS) and HTC's Dream G1 (running Android 1.0), consumers entrust their lives to mobile devices. In a 2015 survey conducted by the Pew Research Center, 92 percent of people in the United States owned a cellphone, and 68 percent owned a smartphone. PEW RESEARCH CTR., DEVICE OWNERSHIP (2015). That averages out to almost one mobile device per person in the United States.

How does this effect law enforcement? With mobile devices allowing consumers to communicate, socialize, bank, shop, navigation, start their car, track their health, and monitor their in-home surveillance cameras, a plethora of information is contained on these devices. Just about every crime being committed has the potential to have the involvement of a mobile device, but the investigation team must first recognize the mobile device—whether it is a watch, phone, or tablet—and then preserve the data for collection and analysis. While it is getting more difficult to bypass security features in mobile devices, the Cybercrime Lab can assist you in determining your options.

II. Preservation of data

For all investigators, identifying and preserving data is the goal when seizing digital evidence. This can be more difficult when dealing with mobile devices that have their own distinct challenges different from the laptop and desktop computers. One challenge is knowing what to look for. With

smaller and novelty devices on the market, such as the BMW style key fob mini phone, it makes identifying the devices more difficult. Another challenge is collecting all of the data. While mobile devices store a lot of data, the extraction of data from the device may be missing important evidence. Not all data is stored on the device, even though the user has access to the data. With the ease of cloud computing, companies such as Dropbox, Microsoft One Drive, and Google Drive provide the user with capabilities to create, transfer, receive, and delete data in the palm of their hand. While the user may have access to this data from their mobile device, it may not be recovered during extraction and analysis due to data being stored in the cloud or on remote storage. Therefore, it is imperative for the investigative team to determine what web-based email accounts, social media accounts, and file storage the user may have so the accounts can be preserved. This data, along with the extracted data from the mobile device, could paint a better picture of what occurred during a timeframe.

III. Extraction

One of the most common questions received in the Cybercrime Lab is if the data can be extracted. This is an ever-changing answer because locked devices that cannot be unlocked today may be unlocked next week. As tools vendors work at developing methods to acquire data from devices that are unsupported, they release updated versions unlocking and decoding new devices several times a year. These updated versions may support a device sitting in evidence collecting dust. It is recommended that stored evidence items should be re-evaluated every few months to see if they are covered in a released update. If the device is not supported with commercial tools, you can contact the Cybercrime Lab (cybercrimelab@usdoj.gov) for assistance in determining what options are available. The lab will ask you to provide the make and model number from the device, operating system if known, and the carrier (i.e. Samsung, SM-G900P, Android 5.1, Sprint).

There are different levels of data extractions from mobile devices, just as with computers. Some allow for further, deeper analysis, and some do not. Knowing which type of extraction was completed is important and can be derived from the report. The three common extractions are Logical, File System, and Physical.

A Logical extraction is the quickest of extractions, and extracts the data through issued API (Application Programming Interface) commands. The commands allow the device to return the requested information from the device, such as the contents of SMS, call logs, and media, but not typically data from the third-party applications. Typically, the File System extraction will include the file structure of the device, collecting the folders, sub-folders, and their data. This generates more data than the Logical extraction, and can be used for further examination—the deep dive. The Physical extraction is the most comprehensive of the extractions. This will provide a bit-for-bit copy of the device's flash memory. With this, you will have the entire memory capture, including the unallocated or deleted space and hidden system files that the user does not see.

With locked devices, the Cybercrime Lab uses various techniques and tools to acquire the data. If your device is listed as unsupported, contact the Cybercrime Lab at Cybercrimelab@usdoj.gov for assistance.

IV. Analysis

One key benefit in obtaining a file system or physical extraction is the ability to perform advanced analysis of the device data. This includes the data contained inside the applications, more

commonly called apps, that are installed on the device. Apps are self-contained software programs either pre-installed or user installed on the device to run programs such as messaging, GPS, social media, and web browsers. The data in these apps is typically stored in SQLite databases and often contains valuable information.

During the analysis of the data, SQLite databases on the device are identified by their file header, 0x53514C69746520666F726D6174203300. The known databases are identified, decoded, and presented to the examiner in a readable, organized format. In commercial tools, the data is read from the SQLite databases and separated into unique sections—such as SMS, Call Log, and Contacts—for the end-user. Known databases are those that the tool has been programmed to recognize and understand how the data is stored. The commercial tools support and decode thousands of different apps, including the popular social media, communication, file storage, and mapping applications, but the databases may need to be exported for further analysis.

What if the entry or data was deleted? Depending on the configuration of the database and its associated files, the data may be recoverable. Some SQLite databases have associated WAL, or Write-Ahead Log, files to assist in writing data to the database. As entries are written by the user, such as a contact entry or SMS message, they are first written to the WAL file. The database will check for the most current data, which either resides in the database or in the WAL file. The data is then moved from the WAL file to the database once the database has completed a normal shutdown. But is the data still in the WAL file? Yes, it could be. SQLite forensic tools, such as Sanderson's SQLite Forensic Suite, allow examiners to search the database and the WAL file for deleted entries that are no longer visible to the user and some commercial tools.

To help explain this, here is an example: if there were five contacts in the Contacts_2.db (.db signifying a database) and I deleted one, the database itself would only see the four remaining entries. If I add a new contact entry but the database failed to close properly, I would still have only four entries.

The new entry would have been in the WAL file, and if the tools failed to process the WAL file, the data could have been missed. However, if I allow the new entry to be added into the database, this could overwrite old data that was present and set to be updated with the new entry. If there is a question about data, or missing data, from a database, and there is an accompanying WAL file, the best practice is to use tools designed for SQLite analysis. A deeper dive into the database may recover old entries that are no longer seen by the database, as well as possibly indicate when the entry was present.

Other challenges with mobile devices are the number of different apps and ensuring that those apps are being supported in the report. We discussed above about "known" databases, but what about unknown databases, those that are not supported for decoding. An example of data not being decoded occurred during the analysis of a physical extraction from a Samsung device. The analysis for Blackberry Messenger revealed a Blackberry Messenger database at this file path: /Root/data/com.bbm/files/bbmcore /master.enc. The database was not decoded due to the database being encrypted, evident by the master.enc file and the data being unreadable (hexadecimal, 0xF6F7CBD9CC1E1D8933392F, which translates to "……..30/"). The physical extraction allowed for the recovery of the keys to decrypt the database, and once it was decrypted, the database file signature was visible (0x53514C69746520666F726D6174203300 translated to SQLite format 3), and it revealed 1,579 chat messages.

V. Conclusion

Mobile devices contain more than just call logs and text messages; they contain a plethora of information, some in the device and some in the cloud. Working with the investigative team to locate and preserve the cloud and web-based accounts will help provide a better picture of the subject's life.

With your locked devices, remember that if it is not supported today, check back or contact the CCIPS Cybercrime Lab for updates and possible solutions. With this ever-changing time, devices not supported last week could be supported next week.

Most mobile device forensic reports come with a list of application SQLite databases identified on the phone. This list needs to be reviewed to see if the database was decoded. While it is not common for commercial tools to miss supported databases, an update from the app builder could influence whether the tool worked properly. Third-party tools can assist in looking deeper into databases if the need arises. If you need assistance with your mobile device, contact the CCIPS Cybercrime Lab for assistance at CybercrimeLab@usdoj.gov.

ABOUT THE AUTHOR

❑ **Daniel Ogden** is a Senior Digital Investigative Analyst in the CCIPS's Cybercrime Lab. He has over 22 years of law enforcement experience and 12 years in the computer crime profession. He is a Cellebrite instructor and specializes in mobile device analysis and computer forensics. He previously served as a Computer Crime Investigator with the Brevard County Sheriff's Office and served 11 years on federal task forces investigating computer related crimes.

The Cybercrime Lab is a group of highly trained digital investigative analysts located in the Computer Crime and Intellectual Property Section of the Criminal Division in Washington, DC. The Cybercrime lab provides support to prosecutors through advanced digital investigative analysis, technical and investigative consultations, and research and training in support of Department of Justice initiatives.

Decrypting a Predator: The Investigation and Prosecution of Steven Rockett

Paul T. Maloney
Assistant United States Attorney
District of Oregon

Gary Y. Sussman
Assistant United States Attorney
Project Safe Childhood Coordinator
District of Oregon

I. Introduction

On the surface, 44-year-old Steven Rockett was a model suburban single parent. His mother and two sons lived with him in a large home he built after his divorce. He was a devoted father. He was the unofficial team photographer for his sons' baseball teams. Other parents trusted him.

Rockett's home was the hub of social activity for his boys and their friends. There was a pool table and a full-sized pinball machine. Sleepovers with late night gaming were routine. From all appearances, Steven Rockett was a cool dad. Below the surface, however, he was a predatory child molester with a long history of sexually abusing and exploiting young girls and boys, both here and abroad.

Rockett's façade began to crumble when his ex-wife, with whom he was embroiled in a custody dispute, raised concerns about his behavior with children in her native country of the Philippines. A few months later, in August 2013, investigators learned of allegations that Rockett had sexually abused a 13-year-old girl who had been staying at his house. Thereafter, investigators serving a search warrant at Rockett's house made an eerie discovery: a tiny video camera hidden in the wall of an upstairs bathroom, strategically positioned to capture images of naked children in the bathroom and wired (via the ceiling crawlspace) to a small digital recorder in Rockett's bedroom. They found two other surreptitious recording devices as well, which would eventually play a pivotal role in the investigation.

Upon further investigation, law enforcement officers learned that Rockett had a sophisticated computer system with multiple data storage devices. He went to great lengths to secure his system. He used an anonymizing web browser, file wiping software, evidence eliminating software, and two separate encryption programs. An external hard drive connected to his computer was fully encrypted. Steven Rockett confidently told investigators, "*You won't find anything on my computer*."

What began as an allegation of sexual misconduct by a bitter ex-spouse and a delayed report of sexual abuse by a troubled 13-year-old girl soon grew into a multi-jurisdictional, international investigation. What emerged was a troubling and persistent pattern of grooming, sexual abuse, and sexual exploitation of boys and girls in both Oregon and the Philippines.

Multiple victims told similar stories of their encounters with Rockett. They described how he befriended them and promised them gifts and special treatment in order to gain their trust. He induced them to engage in increasingly sexualized behaviors. He encouraged them to take showers, during which he photographed them both with and without their knowledge. The encounters often culminated in hands-on sexual abuse. Rockett abused and exploited boys and girls—some as young as eight years old.

This case presented a number of formidable challenges: the scope of Rockett's crimes against scores of children; Rockett's technological sophistication and the lengths to which he went to conceal evidence of his crimes; the degree to which he manipulated his victims in order to thwart the investigation; and the substantial logistical difficulties involved in identifying victims who lived in the Philippines and securing their testimony at trial. In the end, despite those challenges, Rockett was successfully prosecuted in both state and federal court. He will spend the rest of his life in prison. He will never harm a child again.

II. Investigation

The investigation began in March 2013, when Rockett's ex-wife reported concerning behavior she had witnessed during their marriage. They met in the Philippines in 2000 and were married later that year. They traveled to the Philippines together several times so she could visit her family. She described how Rockett would "get kids" in her hometown of Cebu City and take them to a hotel room. One day, she followed him and a group of children to a hotel room, where she found them partially naked. He claimed they were just playing "strip poker." She identified the children she saw, many of whom were local neighborhood children, from a photo recovered from defendant's public Flickr account.

Rockett's ex-wife said that other family members told her about instances of Rockett engaging in sexually inappropriate conduct with children in the Philippines. She reported seeing child pornography on defendant's computer. Several weeks later, Rockett's ex-wife reported that Rockett had communicated with her sister in the Philippines via Facebook, soliciting the sister to produce sexually explicit images of children (including the sister's own daughter) and email them to him.

Investigators recovered Facebook records documenting communications between Rockett and others in the Philippines, including his former sister-in-law. Rockett offered to send money or gifts, such as cellular telephones and digital cameras, in exchange for naked photos of children. He was specific in his requests, insisting on images that showed the children naked, "front and back," and "no shy."

In August 2013, a second investigation began when a teenage girl, *NS*, told her mother that Rockett had raped her. Initially, *NS's* mother did not believe her. Rockett, after all, was a trusted family friend they had known for years, who offered to house *NS* and her two older sisters when *NS's* family was homeless and destitute. The disbelief vanished, however, when *NS* showed her mother Facebook chats during which Rockett pressed *NS* to take naked "selfies" using a smart phone he had purchased for her. The mother later learned that Rockett had also exploited and abused her other two daughters.

NS described in chilling detail how defendant sexually abused her, how he produced sexually explicit images of her, and how he photographed himself engaged in sexual acts with her. *NS* watched

him take the memory card from his camera and put it into his computer. He never showed her any of the actual photos, however.

Investigators obtained a warrant to search defendant's home. They seized computer equipment; expensive, professional-grade camera equipment; the camera hidden in the bathroom wall; the two additional hidden cameras; a variety of data storage media; and a slew of cellular telephones. Investigators hoped that the digital evidence would corroborate the statements of *NS* and her sisters and would provide compelling evidence of Rockett's crimes.

Rockett, however, was computer-savvy. He secured his digital media in order to avoid detection. He used Tor to browse the internet anonymously. He used file wiping software to remove his internet history, securely delete all cache memory, and overwrite deleted files in the unallocated space on his hard drives. He had installed two separate encryption programs with complex, multi-level passwords. One of those programs utilized steganography—hiding files within other files. An external hard drive was fully encrypted. Forensic examiners tried unsuccessfully to decrypt the drive. They found no contraband images of *NS* or her sisters.

Examiners from the Northwest Regional Computer Forensics Laboratory *did* find evidence of nefarious conduct on some of the other devices, though. Examiners found remnants of surreptitious recordings of naked children showering and using the bathroom in unallocated space on the memory cards from the various hidden recording devices found in defendant's house. The memory card in one of the devices (a clock radio that contained a tiny video recorder) revealed video clips of what appeared to be Filipino boys and girls showering and using the toilet in hotel bathrooms. Some of the clips depicted those children engaged in sexual conduct with Rockett. In one of the clips, Rockett is shown using a small digital camera to photograph a young-looking Filipino performing oral sex on Rockett. Examiners also found remnants of video clips from a video editing software program on one of Rockett's computers. The remnants, which appeared to have been captured by a hidden camera, showed a *different* set of adolescent boys showering and using the bathroom in what turned out to be defendant's *former* residence.

The prosecution teams faced two perplexing cases—a state case that had victims but no digital evidence to corroborate their accounts of hands-on sexual abuse, and a federal foreign sex tourism case that had compelling digital evidence but no identified victims. Federal prosecutors and the FBI partnered with state prosecutors and local law enforcement officers to identify all of Rockett's victims and prosecute both cases.

Local investigators scoured through thousands of pages of Facebook records and thousands of snapshots of children found on unencrypted drives on Rockett's computers and in his cloud storage accounts. They learned that Rockett often hosted sleepovers at his house for his sons' baseball teammates. The boys described how Rockett insisted that they all take showers before going to bed at night, and again in the morning. Several of those boys were identified in the surreptitious bathroom recordings. Many initially denied that Rockett had touched them. Several eventually disclosed that he overtly photographed and fondled them while they showered. Some later recanted their reports or gave conflicting accounts in follow-up interviews.

Meanwhile, the FBI initiated a foreign sex tourism investigation. They gathered travel documents and hotel and credit card records. With little more than the photo identifications from Rockett's ex-wife

(who refused to cooperate with the investigation after his arrest) and an address gleaned from the background of a photo from Rockett's Flickr account, FBI agents traveled to Cebu City, Philippines, in an attempt to identify and interview victims. Over three days, agents located and interviewed a number of victims, each of whom described disturbing interactions with Rockett. A few spoke English. Some spoke Tagalog. Most spoke only Cebuano, the local dialect. A local police officer acted as an interpreter.

The children explained how kids from the local neighborhood, or "barangay," would line up to receive 100 peso notes—a little more than $2—from Rockett. He took them to the beach or shopping at a local mall. They accompanied him to his hotel, where they swam in the hotel pool, took hot showers, sat on a big, comfortable bed, and watched cable television—real luxuries for children who lived in abject poverty.

They described how Rockett cajoled them to take showers in the hotel bathroom. Once they were naked, he took photographs of them. Several described acts of molestation, including fondling and oral sex. They described the gifts and compensation Rockett gave them in exchange for those sexual encounters.

Some of Rockett's Filipino victims were young adults by the time they were interviewed by the FBI. Some were still children. Most lived in the same barangay; all were aware of Rockett's arrest. Many were unwilling to travel to the United States to testify. Rockett, as it turned out, was still held in high esteem within the barangay.

Meanwhile, forensic work on Rockett's digital devices continued. From Rockett's primary home computer, they determined that Rockett had downloaded images of child pornography from a website in the few hours between the last time he ran a file wiping program and his arrest on state charges. Those images, which were found in a compressed ".rar" file, would form the basis of the possession count in the federal trial.

Since Rockett's primary home computer was the device that had the encryption onboard, investigators requested a full analysis of other computers found in the home. Using a keyword search for encryption related terms, examiners sought information related to Rockett's use of encryption. On a computer that ostensibly was a gaming computer for the kids in the home, examiners recovered fragments of online conversations from the unallocated space on the hard drive. The conversations were portions of "Flickr chats" between Rockett and others discussing encryption and how it could be used to prevent the government from detecting the distribution of "special" images transmitted over the internet. Combing the data from this email cache, examiners recovered thumbnail images of photographs of young Filipino looking children from an obscure email cache associated with Rockett's email address, which established that Rockett's email program had handled these images. These small pieces of digital evidence scoured from many different devices were persuasive evidentiary nuggets that put many of Rockett's activities into context.

III. Prosecution

Rockett was initially charged in Oregon state court with the sexual assault of *NS* and her sisters. As the investigation progressed, more victims came forward, and more evidence was recovered. Rockett posted $350,000 bail for his release on the state charges. In order to preserve the federal interests relating to his online and overseas activities, a complaint was filed in federal court for Attempted Production of Child Pornography in violation of 18 U.S.C. §§ 2251(c) and (e). Rockett was detained on the federal

charges after his initial appearance in federal court. Shortly after that, Rockett violated the terms of his state release by contacting minor victims from jail.

Ultimately, Rockett ended up in federal court, where he was indicted in five counts of producing and attempting to produce child pornography, in violation of 18 U.S.C. §§ 2251(a), (c), and (e); two counts of engaging in illicit sexual conduct with a minor in a foreign place, in violation of 18 U.S.C §§ 2423(c) and (e); and possession of child pornography, in violation of 18 U.S.C. §§ 2252A(a)(5)(B) and (b)(2). A Petite Policy waiver was not sought because all but one of the charges involved different victims, and for the one victim common to both cases, the incident dates differed by a period of three years.

After a lengthy and difficult trial, Rockett was convicted in state court of multiple counts of second degree rape, second degree sodomy, first degree sexual abuse, using a child in a display of sexually explicit conduct, and invasion of privacy—all stemming from the sexual abuse and exploitation of *NS*, her sisters, and two other children. He was sentenced to over 52 and a half years in the Oregon Department of Corrections. However significant this sentence was, it did not provide a measure of justice for the crimes committed against all of Rockett's overseas victims. Steven Rockett refused all efforts to negotiate his case.

As the federal case progressed to trial, unique and complex challenges arose with respect to the government's foreign witnesses. The witnesses faced intense pressure from friends and family members to not cooperate with the prosecution of Steven Rockett. Many were unwilling to travel to the United States for the trial. One had moved and could not be located. Those who were willing to testify lacked both birth certificates and passports. Obtaining those documents required a monumental effort.

The FBI's Assistant Legal Attaché (ALAT) in Manila, assisted by a Portland Division agent detailed to the Philippines, went to extraordinary lengths to help the victims and their guardians secure the necessary travel documents. The minor victims could not obtain passports until a parent or guardian obtained one. The parents, in turn, could not obtain passports without a birth certificate, which almost none of them had. And birth certificates could only be obtained from local officials on the island on which the parent was born. In one instance, that meant a trip from Cebu City to a small island in the province of Masbate, rife with anti-American terrorist activity. Alerted that a terrorist group was actively looking for them, the agent, the guardian, and their Philippines National Police escort fled the island under cover of darkness in a motorized sea kayak. After a harrowing two-hour open ocean transit followed by an overland trip to the city of Legazpi, they were safe.

Once the necessary travel documents had been secured, the FBI prepared applications to parole the victims and their guardians into the United States for trial. The paroles came through shortly before the victims were scheduled to board the plane for the United States. Because they were entering the country on special paroles rather than on visas, FBI agents had to escort the Filipino witnesses everywhere they went—24 hours a day.

Meanwhile, prosecutors faced a slew of pretrial motions. Rockett sought to exclude evidence found recovered in cache files, in unallocated space, and in the deleted files folder of his computer equipment. He moved to exclude evidence of the limited statements he made following his arrest. He sought to exclude evidence found on the memory cards for the devices containing the hidden video

cameras, and the video recorder connected to the pinhole camera hidden in his bathroom. He also moved to exclude evidence of his state court convictions.

The government sought to admit all of that evidence, except for Rockett's statements (which were equivocal at best). After conducting an in-depth balancing test under Federal Rule of Evidence 403, the district judge admitted evidence of defendant's state convictions under Rule 414 and permitted the government to introduce images and videos recovered from the various devices and memory cards. However, the court ruled that it would limit the amount of child pornography images that would be presented to the jury. The court wanted to avoid overwhelming the jury and thereby unduly prejudicing Rockett.

That limitation ended up being a blessing in disguise. Because of the court's limitations, the government was able to winnow down the images to the most egregious content, maximizing its impact on the jury. The video footage from the hidden cameras contained hours of non-offensive images interspersed with moments of shocking displays of lewd and lascivious conduct. Rockett's motion had the unintended consequence of requiring the government to cherry-pick the most offensive images to offer at trial. First, the court reviewed all of the images and videos the government intended to offer. *See United States v. Curtin*, 489 F.3d 935, 957 (9th Cir. 2007) (en banc) (stating that prior to determining admissibility, trial court required to review entirety of government's proffered evidence as part of Rule 403 analysis), the court found that the "contraband evidence is not greater than necessary to show [Rockett's] identity, intentions, absence of mistake, and allegedly unlawful conduct."

With trial preparations in full swing, the FBI sent agents to escort the Filipino witnesses to the United States. Three interpreters were hired—two for court translation and a third who assisted the victim services team. The victim services interpreter was from Cebu City, worked in a Portland-based non-profit, and spoke both Tagalog and Cebuano. She accompanied the FBI to Cebu City and traveled back to Portland with the victims and their guardians. She provided much more than just translation services for the victims; she was a helpful and calming presence as they traveled halfway around the world to confront their abuser.

At trial, the Filipino victims testified in a clear, consistent, and compelling manner. Their accounts of Rockett's manipulation, abuse, and exploitation meshed almost seamlessly with similar accounts given by Rockett's victims here in the United States. In fact, the investigation was so thorough that the defense characterized it in their closing argument as an "open checkbook investigation," and a "spare no expense" prosecution. The government responded by demonstrating how those extraordinary investigatory efforts were necessary to counter the sophisticated steps Rockett had taken to manipulate his victims, to conceal evidence, and to avoid detection.

The government was forced to dismiss one of the foreign sex tourism counts after a victim—whose testimony was essential to proving the elements of that count—decided at the last minute not to travel to the United States. The jury convicted Rockett on all remaining counts. The court agreed with the government's argument that Rockett deserved a separate and distinct sanction for each of his victims and sentenced him to a total of 60 years' imprisonment in the federal case, of which 45 years was imposed to run *consecutively* to his undischarged state sentence.

IV. Successful Strategies for Overcoming Encryption at Trial

Foreign sex tourism cases are challenging under the best of circumstances. They are even more challenging where the defendant encrypts his data, conceals or destroys evidence, and attempts to manipulate witnesses.

It is difficult to identify and locate victims in foreign countries. Language and cultural barriers make interviewing difficult. There are often no child advocacy centers and no trained forensic interviewers. It is frequently up to the case agent to conduct the interviews, and even then, interviews are subject to local laws, regulations, and police practices.

Convincing victims and their guardians to travel to the United States is no easy task. Even if they agree to do so, there are considerable logistical difficulties. Obtaining necessary travel documents can be time consuming and frustrating. Arranging for entry into the United States involves multiple bureaucratic hurdles. Travel logistics for agents, victims, their guardians, and interpreters can be daunting and expensive. And, of course, any assistance we provide in obtaining travel documents and providing travel arrangements is discoverable *Giglio* material. But in the end, it was all worthwhile.

At trial, a number of the victims recounted the nightmares they have endured as a result of Rockett's abuse. Some recounted the pressure and ridicule they faced from friends, neighbors, and even family members who remained loyal to Steven Rockett. Some testified that they came forward so that other children would not be victimized. Their courage and resolve were palpable.

Steven Rockett tried to conceal the digital evidence by encrypting it and by using wiping software. But encryption did not end the case, even though forensic examiners were not able to defeat it. Through diligent investigation and thoughtful preparation, the prosecution still succeeded. Here are some of the strategies that worked in our case. Hopefully, they will work for you as well.

- Strongly encourage federal agents to work hand-in-hand with state and local investigators. Evidence developed during the federal investigation was pivotal in the state prosecution. Evidence developed by state investigators helped to cement the federal case. Testimony from local victims helped to corroborate the testimony of the Filipino victims. Make it a team effort from start to finish.
- One of the state prosecutors was cross-designated as a Special Assistant United States Attorney. He was instrumental with the federal case from the beginning. That prosecutor played a key role in overseeing both investigations, marshalling the evidence, and devising trial strategies in both cases.
- Be creative in how and where you look for evidence. Draft search warrants to look for all kinds of data that is potentially relevant to prove the crimes under investigation. User identification and attribution evidence is nearly always relevant.
- Comb the residual data (caches, history, unallocated space, etc.) for any tidbits of useful information. Much of the digital evidence against Rockett was found in those very places. Evidence found in places Rockett was unaware of provided useful threads for investigative follow-up.

- Identify who encrypted the device and present reasons why that person hid their digital activities from law enforcement and others. Pay attention to data that was *not* encrypted as well. Rockett, for example, tried to argue that there were many legitimate reasons to encrypt data, such as safeguarding tax returns and financial records and protecting attorney-client communications with his divorce attorney. As it turned out, however, Rockett's tax returns, financial records, and attorney-client communications were *not* encrypted. Thus, the jury was left to infer that Rockett used encryption for a nefarious purpose.
- Take extraordinary steps to identify and interview witnesses, especially if the witnesses are overseas. Keep language barriers and cultural differences in mind. If possible, have the agent take a forensic interviewer along, and arrange for a bona fide translator to assist with the interviews. Using a local law enforcement officer as an interpreter can create problems at trial, especially if it appears that the local officer was interviewing victims or witnesses rather than simply translating what was said to and by your case agent.
- Coordinate with the ALAT in the foreign country early in the investigation. The ALAT was critical to laying the ground work with local authorities in order to conduct investigative operations in the foreign country. Some countries restrict how witness interviews are conducted, whether interviews can be recorded, and whether all questions must be asked by a local official. The ALAT also served as a consistent local point of contact for victims and witnesses and assisted in securing their travel documents.
- Commit a temporary duty agent from the home division running the investigation. As good as our ALAT was, he did not have the bandwidth to accompany our many victims and witnesses through the bureaucratic maze of the Philippines. Having a temporary duty agent on the ground in the foreign country was highly beneficial in a number of respects. The home office agent was intimately familiar with the needs of the investigation and prosecution, and he focused his efforts in the foreign country to achieve these objectives. The agent provided continuity for the victims and witnesses. They knew and trusted him, he knew what he needed to accomplish to get them on the plane to the United States, and he knew where each witness was in the process.
- Document all compensation paid or provided to witnesses. Things like covering the costs of obtaining birth certificates and passports, transportation to and from government offices to obtain those documents, meals and lodging expenses, transportation to and hotel costs in the United States, per diem payments, and the like must be documented and disclosed. Own the fact that these expenses were necessary to facilitate the witnesses' attendance for trial. Argue that this is one reason why offenders go overseas to commit their crimes.
- Identify the manner in which your witnesses will enter the country. Know the steps and timelines required for your overseas witnesses to obtain a visa/parole permitting entry into the United States.
- Partner with all available agencies and resources. CEOS provided invaluable advice and assistance in securing funds for victim travel. We were fortunate that one of our agents was detailed to FBI Headquarters during the lead-up to trial. She was able to advocate for our case within the FBI and was a key liaison with the Major Case Coordination Unit (MCCU). The MCCU supported agents in the Philippines who provided timely advice and assistance in securing our foreign witnesses for trial.

- Make sure you have interpreters lined up at each step in the process—initial and follow-up interviews, transportation to the United States, pretrial preparation sessions, the trial itself, and while witnesses are waiting to testify.
- Reach out to non-governmental organizations or members of the community who are familiar with the language and culture of the foreign victims and witnesses. Such third parties can help victims and witnesses feel more at home, can help arrange for familiar foods and activities, and can help relieve the stress and pressure of traveling to a foreign country to confront a sexual abuser.
- Cooperate. Coordinate. Communicate. From the outset of the investigation, many different agencies worked closely together to determine the scope of Rockett's criminal activities. No one individual or agency could have managed the innumerable details of a multi-victim global investigation. Teamwork and clear communications across multiple time zones was not easy, but were key elements to the success of this complicated foreign sex tourism investigation.

V. Conclusion

Encryption need not mean the end of your investigation. Thorough analysis of remnant data can generate useful information for investigators and provide important documentation of a defendant's criminal activities. Investigators and prosecutors must be nimble and creative in locating and securing evidence to establish the defendant's criminal conduct and must be willing to go the extra mile to investigate and prove the case. Offenders go to great lengths to hide or destroy evidence of their wrongdoing; we must be prepared to go even farther to ferret out the truth and to hold them accountable for their unlawful conduct.

ABOUT THE AUTHORS

❑ **Paul T. Maloney** currently serves as a federal prosecutor in the District of Oregon, where he prosecutes violent crimes and Indian Country cases. Mr. Maloney began his legal career in 2001 as Deputy District Attorney for the District Attorney's Office in Washington County, Oregon, where he served as a SAUSA and specialized in child abuse prosecutions.

❑ **Gary Y. Sussman** is an Assistant United States Attorney and Project Safe Childhood Coordinator for the District of Oregon. He has been a federal prosecutor since September 1990 and has been handling child exploitation cases since 2006.

Challenges in Modern Digital Investigative Analysis

Ovie Carroll
Director
Cybercrime Lab
Computer Crime & Intellectual Property Section

In the last 15 years, significant challenges have arisen in the field formerly known as "computer forensics." Among these challenges are the dramatic increase in the volume of digital evidence, the rise in use of effective encryption, the creation of new technologies that cause digital evidence to become increasingly evanescent (e.g., ephemeral), and an increased expectation amongst jurists that prosecutors not only prove that evidence was on the defendant's computer, but attribute the evidence to the defendant. This article discusses some of these challenges and identifies techniques that prosecutors, agents, and analysts can consider to effectively respond to these challenges.

I. Introduction

The Cybercrime Lab is a group of highly trained digital investigative analysts located in the Computer Crime and Intellectual Property Section of the Criminal Division in Washington, DC. The Cybercrime Lab provides support to prosecutors through advanced digital investigative analysis, technical and investigative consultations, and research and training to support Department of Justice initiatives. Digital Investigative Analysis (DIA) is the evolution of what was previously referred to as "computer forensics." It is important for prosecutors to appreciate the three aspects of the profession that caused this evolution:

Digital. Digital Investigative Analysts (analysists) no longer limit their analysis to standard computer systems. Today, analysts examine everything "digital," including desktop computers, laptops, mobile devices (cell phones and tablets), GPS navigation devices, vehicle computer systems, Internet of Things (IoT) devices, and much more. We are still in the infancy of the digital age, but developers of many products—from shoes and sports bras to lightbulbs and doorbells—are already incorporating technology into their products to collect, store, and transmit information about the user that they can analyze and hopefully monetize.

Investigative. While technology progresses at lightning speed, the legal system and those who uphold our laws are just beginning to appreciate the need for analysts to conduct deeper "investigative" analysis on digital devices to obtain a better understanding of issues being investigated. Each year we are generating or replicating eight zettabytes of information. That is equivalent to a stack of paper 1.6 trillion miles high. To manage the high volume of data that needs to be analyzed, some organizations have employed a raw data extraction process to digital evidence. This non-analytical approach blindly identifies types of files (e.g. pictures, documents, spreadsheets, etc.) in the storage media, without further

analysis, to determine if the user opened the file or even knew the file was there. This raw data extraction process allows an organization to quickly process a large volume of data and may be an excellent first step in the simplest cases.

Raw data extraction, however, does little to satisfy many of the offense elements necessary to establish guilt. In contrast, DIA requires analysts to investigate or even "interrogate" digital devices. Analysts ask questions in the form of keyword searches and review digital artifacts to form additional questions or logical investigative leads based on the answers received. Even when the response to questions is silence (or a lack of recorded information), an analyst may ask why is there no response or recorded information. Was counter-forensics conducted? Is there something unique about the digital device being investigated that the technique or tool cannot read or display the information?

Analysis. Lastly, an analyst must "analyze" the response to each question and determine its relevance to other digital artifacts, as well as how it relates to information available from the non-digital investigation. An excellent example of this was used in "The Physical Computer and the Fourth Amendment" by acting Principal Deputy Chief of CCIPS, Josh Goldfoot, where he explained that in isolation, the fact that a suspect downloaded tide tables for a particular beach in Oregon at 5 a.m. might mean nothing. Josh Goldfoot, *The Physical Computer and the Fourth Amendment*, 16 BERKELEY J. CRIM. L. 112 (2011). When combined with the fact that a young woman's body was discovered in the surf on that beach an hour and a half later, however, the significance of the tide tables became apparent. *Id.*

II. Incident Response and Encryption

For years, law enforcement has debated the value of imaging Random Access Memory (RAM) when they encounter a powered-on computer with an active user account logged in. RAM is the place in a computing device where the operating system, applications and data in use are kept so they can be quickly reached by the device's processor. RAM is much faster than other kinds of storage. Data remains in RAM as long as the computer is running. When the computer is turned off, RAM information in RAM rapidly dissipates and is lost. In 2016, the majority of law enforcement more often elected to pull the power plug from the computer rather than image RAM.

Many agents still prefer not to acquire RAM because they believe that RAM is unlikely to contain relevant evidence. Sometime agents base this belief on the specific nature of the investigation (e.g., white collar crime) or the latency of the crime under investigation. Today, however, the most appropriate practice is to image RAM where practicable. First, an aggressive defense counsel may argue that RAM might have contained exculpatory evidence and its intentional destruction amounts to a knowing *Brady* violation. Second, today there is increased possibility that the hard drive of the computer to be searched will be encrypted. That possibility is becoming more likely each day.

III. Encryption is default on new computers

Investigative agencies are already beginning to see an increased use of "BitLocker" whole disk encryption. It is not just that our targets are getting savvy about securing their data. In many instance, the providers are doing the work for our targets. For example, starting with the core edition of Windows 8.1, Windows RT, and Windows 10, Microsoft began *automatically* encrypting the system boot volume (typically the entire C-drive) without notifying the user.

Thankfully, as of the writing of this article, whole disk encryption is still not the default on every Windows computer; it is hardware conditional. These conditions must be met for Microsoft to encrypt the operating system drive:

(a) the device meets Connected Standby or Modern Standby hardware specifications;
(b) the device features a non-removable (soldered) RAM (this protects against the rarely used cold-boot technique where RAM is removed and placed in a separate reader device and imaged without allowing the computer to be powered down);
(c) the device has a Trusted Platform Module (TPM) 2.0 chip; and
(d) at least one account with administrative privileges logs in with Microsoft Account credentials (as opposed to using a local Windows account).

While this may sound like a lot of very specific requirements, it is worth noting that every Windows Surface and Surface Pro computer meets all of these requirements and is encrypted by default. And even if a computer does not initially meet all the requirements (e.g., it has no solid-state drive or an account with administrative privileges using Microsoft account credentials is used), the moment the device meets all the prerequisites, Windows will begin silently encrypting the boot partition in the background without notice to the user.

It is important for prosecutors to be aware that because BitLocker Device Encryption encrypts Windows devices without user awareness, it also automatically stores a 48-character recovery key in the users Microsoft OneDrive account. Prosecutors may be able to serve legal process upon Microsoft to obtain the BitLocker Recovery Key from the user's Microsoft OneDrive account. CCIPS recommends that prosecutors use a search warrant to obtain the recovery key in most instances. If you find that any of your personal computers have been automatically encrypted, you can see all your BitLocker recovery keys by logging into your OneDrive account and going to https://onedrive.live.com/recoverykey.

IV. Four Basic Incident Response Steps

With the increased likelihood of encountering encryption, prosecutors and agents should familiarize themselves with the four basic, recommended steps for responding to a computer that is powered on with a user logged in.

First, isolate and preserve the state of the computer as it is when law enforcement first encounter it. Do a visual assessment to determine if anything requires immediate action. For example, consider disconnecting the system from the network. If the responder detects excessive hard drive activity suggesting the drive is being wiped, consider terminating the wiping program if possible or removing power from the computer to prevent further damage.

Second, preserve volatile data by imaging RAM. There are many simple ways this can be accomplished, but all require the introduction of incident response software. Incident response software is

typically introduced to the target computer by inserting external storage media such as a USB drive. Some incident responders have expressed concern that introducing anything to the target computer changes evidence and may render the computer inadmissible. While that is always a theoretical risk, the risk is quite small, and it is usually a greater risk not to image RAM.

As an initial matter, the "changes" to the computer caused by imaging RAM are minimal, contained, and usually identifiable. These changes are especially de minimus when one recognizes that any computer powered on is always in a fluid state of motion, and changes are taking place regardless of what actions are taken by the examiner. Thus, the risk created by imaging RAM is quite minimal. The incident responder can further minimize the risk by using a sanitized storage device to introduce the incident response software and by carefully documenting any actions they take on a live computer system for later reference.

The risk created by not imaging RAM is often much more significant. The average computer sold between 2015 and 2016 came with at least six gigabytes of RAM. Six gigabytes of text roughly equals a stack of paper 6,000 feet high. An aggressive defense counsel may argue that by removing power from the computer without preserving RAM, your agent just destroyed the equivalent to a 6,000 foot stack of information (most of which was surely exculpatory).

Third, once RAM has been preserved, check for signs of encryption. The two most common encryption detection tools are "Encrypted Disk Detector" (EDD) by Magnet Forensics or "Crypthunter" by the Software Engineering Institute at Carnegie Mellon University. When executed, both tools will report the presence of a number of different volume and disk based encryption programs. More information about EDD can be found at www.magnetforensics.com/free-tool-encrypted-disk-detector/. More information about Crypthunter can be found at www.cert.org/forensics.

Finally, create a forensic image. If there are no indications of encryption, and RAM has been successfully imaged, power should be removed from the system to abruptly stop all operations. Removing power prevents any maintenance or counter forensic programs from running and causing changes to the system during the standard shutdown process. A "write block" (preferably a "hardware write block") should be applied to the hard drive before any further actions are taken to prevent the imaging process from writing any information to the drive being imaged or otherwise changing the data being investigated.

Before beginning the process of creating a full forensic image (whether a physical image or a faster "logical" copy), consider creating a "triage" image. Analysts can typically image at 60 to 80 gigabyte per hour. A complete copy (full "physical" image) of a one terabyte drive would typically take between 12 to16 hours. In contrast, a triage image uses a more surgical approach to create a smaller, partial image of high value digital artifacts that can reveal key information. For example, a triage image may alert investigators to online accounts that need to be immediately preserved, or actions recently taken on the computer that may aid in taking immediate investigative actions (e.g. searches conducted, files opened, chat sessions, etc.). Analysis of the high value digital artifacts can then be conducted while the more time-consuming full forensic image takes place.

If encryption is detected or suspected because of step three, incident responders should consider creating a live "logical" image of the computer before removing power. Several tools can image RAM and create images of a live system—one of the most popular is FTK Imager by Access Data, which can image RAM, create both live logical or physical images, and accomplish many additional incident response tasks. While a live logical image is not the preferred method of copying a hard drive, it allows

investigators to capture all the active files in an unencrypted state so that if the encryption cannot be circumvented, at least the active files are available for the investigation.

V. Electromagnetic vs Solid State Hard Drives

Another issue prosecutors and analysts should consider is the impact that new "solid state" hard drives (SSDs) have on DIA. Standard hard drives, also called "electromagnetic drives," consist of platters that spin between 5,400 and 15,000 RPMs and hold positive and negative charges read by the computer as binary data. From this binary data, the computer can read the files and programs that store information and make the computer work. Since the beginning of the computer forensic profession, it has been well known that nothing is ever truly "deleted" from an electromagnetic drive. Instead, when information is "deleted" from an electromagnetic drive, the computer is simply told that the space where that information resides is now available for new files to reside, if that space becomes needed. A file deleted can be recovered forever, as long as no other data is written to the area of the hard drive that file resides.

SSDs change this fundamental principle. The benefits of SSDs include increased speed of access. There is no longer a motor moving a head of a hard drive across a spinning platter to read the polarity of binary data stored on it. As a result, the access to data is instantaneous. With no moving parts, SSDs are also silent, less fragile, and stay relatively cool compared to electromagnetic drives.

One negative aspect of SSDs, however, is the "write endurance." Write endurance is the number of "write cycles" (or number of times data can be written to) a block of flash memory can hold. Once a user has reached the write endurance limit, the disk may become unreliable or unable to use any of the cells. As a result, there is a tendency for repeated writes to eventually corrupt the flash memory, making the SSD partially or completely unusable. SSDs employ two features to reduce this phenomenon and expand the life of an SSD. These features are called "wear leveling" and "trim."

Wear leveling is the process of moving data around on the SSD to prevent any specific area of the drive from wearing out prematurely. When active data is moved to a location marked as being inactive, any data previously in that location is overwritten. This process decreases the time deleted files can be recovered on SSDs because data on the drive is constantly being overwritten.

Trim is used to increase the speed data can be written to the drive. As an analogy, if you think of each cell that holds data on an SSD as a paint can, trim is the process that looks at which cells are holding active files, then occasionally pops the lid on all paint cans that are not holding active data. This increases the write speed because data can be immediately written to a clear, open cell rather than first having to pop the lid and clear the "inactive" or deleted files.

Wear leveling and trim have at least two effects that may relate to prosecutors and analysts. First, the amount of time deleted files can be recovered drops from "indefinitely" on an electromagnetic drive to potentially weeks or months on an SSD. Time is now of the essence for imaging an SSD. If you have reason to believe your target has an SSD, act quickly. Second, when wear leveling or trim occurs, data in inactive cells of the SSD are being destroyed, causing the drive to constantly change. As a result, an SSD with a particular hash value when imaged originally may have a different hash value if the drive is later reimaged because trim or wear leveling may occur during the reimaging process.

Unfortunately, the trim and wear leveling functions are accomplished at the hard drive controller level, and nothing can currently be done to suspend these functions. While some operating systems can invoke trim, disabling it through the operating system does not prevent trim from being initiated by the drive firmware. Even attaching an SSD to a hardware write block will not prevent wear leveling or trim.

VI. What is a hash value?

A hash value is a unique identifier representing a specific data set (for example, a particular file, record, or hard drive). The result, which is generated by an algorithm, is a distinct fixed length alphanumeric string, using a combination of letters and numbers. The following is an example of a particular hash value called an "MD5" hash:

26a981554d7d761230bc7ef3a6645375

Such an algorithm result is sometimes called a hash value, hash sum, checksum, or message digest. A hash value can refer to the hash function calculation for any data set, such as a file, record, or hard drive.

Hash values provide a fundamental role in forensic examinations concerning the review and analysis of data. Analysts can authenticate digital evidence by determining the hash value of the original evidence, making a physical copy of the evidence, and then confirming that the copy has the exact same hash value as the original evidence. If a corrupt or sloppy agent changed even a single character in one Word document saved on a 10-terabyte hard drive after imaging it, the entire drive would have a different hash value. Thus, the fact that two hash values match is powerful evidence that the prosecutor is presenting a perfect image of the original drive.

VII. No such thing as a full forensic analysis

As the digital age matures, the number of devices collecting and storing information, and the volume of digital evidence to be examined in any investigation, are becoming a significant challenge. Over the past 15 years, the maximum capacity of a single storage device has doubled every 12 to 18 months. As the maximum capacity of individual devices has dramatically increased, the cost of storage has considerably decreased. The substantial volume of data has had a considerable impact on investigative agencies and their efforts to keep up with the tsunami of digital evidence to be analyzed. One major change to the digital investigative analysis profession is that there is no longer such a thing as a "full forensic analysis."

For years now, the most sophisticated analysts have applied a phased approach to digital analysis. The phased approach consists of a variant of at least three phases: Triage, Identification, and Deep Analysis.

Partially because of the increased storage capacity of individual devices, and secondarily because the investigative value of information tends to decrease with time, the timing of the triage phase is often critical. The earlier triage can be conducted, the more potential value the information may have, whether it is used to confront a suspect in hopes to obtain a confession, or to identify other critical time sensitive evidence that needs to be preserved (e.g. web-based email, storage, or social networking accounts).

Another change occurring in the digital investigative analysis profession is the shift from analysis being conducted by a single examiner, to a team approach. In addition to a phased approach, the SANS Institute Digital Forensic and Incident Response (DFIR) program have conducted extensive research over

the past six years, constructing teams of three, four, and five analysts. The teams were given a forensic image and approximately six hours to identify and analyze digital artifacts and present their findings. A four-person team was found to be the optimal size to efficiently conduct a collaborative analysis of digital evidence. Focusing on high-value digital artifacts, also called "compass points," analysts can quickly reconstruct events that occurred.

VIII. Compass Points or High Value Digital Artifacts

Often, when supporting an investigation, it is helpful to focus on compass points that help prove particular elements of the investigation. This section will highlight some of the compass points that are frequently of most value. This is not an exhaustive list, but only a few of the most valuable digital artifacts in each category.

The information below is provided so prosecutors will have a general awareness of the type of information that may be available through digital investigative analysis. Prosecutors should not use the information below as a "checklist" or "to do list" when working with agents or analysts. As digital artifacts can change with every operating system update or patch, the Cybercrime Lab is available to discuss and consult on any digital evidence matter and can be reached by calling CCIPS at (202) 514-1026 and asking for any available digital investigative analyst.

IX. Location information

NetworkLists Signatures and Profiles — Since connecting to a network is generally proximity dependent, that is, you must be within the range of the wired or wireless network to connect to it, one easy way to prove a computer was at a specific location at a specific time is to identify when the computer was connected to particular networks. The most valuable artifacts that document the networks to which a computer connected are in the "Windows Software registry hive." The Windows registry is essentially several databases that track system and application configuration information, as well as user activity. Although additional registry keys exist, two registry keys in the Software registry hive track every network to which the computer has ever connected. The "\Microsoft\Windows NT\CurrentVersion\NetworkList\Signatures\Unmanaged" key tracks the network description, the MAC address of the default gateway router, and the domain name of each network to which the computer ever connects. It also records a profile "global unique identifier" (GUID) for each network. The "\Microsoft\Windows NT\CurrentVersion\NetworkList\Profiles" registry key tracks all profile GUIDs and for each network. It records the date and time the computer first and last successfully connected to each network and how the connection was made (e.g., wireless, wired, 3G, etc.).

A MAC Address, short for "Media Access Control" address, is a hardware address that uniquely identifies each node of a network, similar to a serial number. Because MAC addresses serve like a unique serial number for each wireless router, you can search available databases to attempt to identify each router's geolocation. By default, all Apple and Android phones are configured to routinely scan for wireless networks around you and collect the network names and MAC addresses (along with other information) and send the collected information (along with your phones GPS location) back to Apple and Google, which use this information to provide you and others with quicker and more accurate

location information. If you ever turn off your WiFi antenna on your Apple or Android phone and then use any application that queries location services, this is why you will receive a notification informing you that you can receive more accurate location information if you turn on your WiFi antenna. A free open source database frequently used to look up the location of a network MAC address is www.wigle.net.

Event Logs — While the software registry hive tracks the first and last successful connection to each network, Microsoft started keeping more robust Windows event logs starting with Windows Vista. The "WLAN-Autoconfig" event log creates an event ID-8001 record with the network name and MAC address for each successful connection to a wireless network. An event ID-8002 record is created and records each unsuccessful wireless connection attempt (e.g., the user does not have the password or types it incorrectly). If a user attempts to connect to the Internet without a proper network connection, Windows will offer to diagnose the problem. If the user agrees to the diagnostics, an event ID-6100 record is created and records the name, MAC address, network name, and signal strength for every wireless network the computer can see at that point in time.

SRUM — An additional lesser known digital artifact that tracks networks to which a computer is connected is the "System Resource Usage Monitor" (SRUM). Starting in Windows 8, Microsoft began monitoring system resource usage and recording that information in an "extensible storage engine" (ESE) database called SRUM. SRUM records each network to which the computer is connected, the network name, the connection start time and duration, the user account responsible for the connection, and the volume of network activity from all applications running (even if the application is not installed on the computer and runs from an external USB drive). SRUM collects and documents this information on an hourly basis, so an examination of SRUM data would allow you to determine within 59 minutes which applications were running and how much data each application transferred (uploaded or downloaded) across the network.

In addition to using SRUM to identify when a user connected to a specific network and for how long, SRUM data may be evidence of an employee transferring mass amounts of data from the corporate network to her laptop before leaving the company. This activity would likely appear in SRUM as the Windows Explorer application transferring the large amount of network data inbound to her computer. If the employee then went to the local coffee shop, connected to her wireless network and uploaded the data to a web-based storage location (like Dropbox), SRUM would show the large outbound network transfer (likely proportionate to the inbound transfer on the corporate network) on the coffee shop wireless network connection. The SRUM Database is located in the "C:\Windows\System32\sru\" directory.

X. File knowledge and access

Windows Searches — For years, one challenge in digital investigative analysis has been proving a user not only had something significant to an investigation on their computer, but that he knew it was on there. Two of the easiest ways help prove knowledge of a file is to prove the user was searching for it or accessed it. In order for Microsoft to enhance the user experience, Windows tracks the names of files you access and search for in multiple locations. As previously discussed, the Windows registry is essentially several databases called registry hives. Each user has his own primary registry hive called the NTUSER.DAT. This registry hive tracks information specific to each user's activity and preferences. Starting in Windows 7, when a user conducts a search on his computer using the Windows search function or the "Charm Bar" in Windows 8-10 (the magnifying glass that appears when you move your mouse to the right edge of the screen), Windows records each search in temporal order in the

"NTUSER.DAT\ Software\ Microsoft\ Windows\ CurrentVersion\ Explorer\WordWheelQuery" registry key. Because the searches are recorded in temporal order, an analyst can frequently see indications of the user's thought process as he searched for particular files.

File Access —– Windows also records in numerous artifacts when a user opens or attempts to open non-executable files. Four of the most useful digital artifacts to identify files opened or attempted to be opened are "LNK" files (pronounced as "link" files), Jump Lists, and several "most recently used" registry keys.

LNK files — A LNK File is an artifact that has existed since Windows XP. LNK files are also known as a "Windows Shortcut" files and are created anytime a user opens or attempts to open a non-executable file. A LNK file is created even if the file opened is on a network or external drive. When an opened file is later deleted, its LNK file does not get deleted with it. Windows creates and stores approximately 149 LNK files in the user's home directory under the "AppData\Roaming\Microsoft\ Windows\Recent" directory. LNK files contain a wealth of information including the modified, accessed, and created dates and times of the file opened; the full directory path, volume name, and volume serial number from which the file was last opened; and the file size.

Starting in Windows 10, Microsoft added rules to when LNK files would be created in addition to when files are opened. On earlier versions of Windows 10, a LNK file was created for the directory to which any file was copied. The creation of a LNK file for the directory a file was copied to was stopped on later versions of Windows 10. However, on versions as early as version 1607, Microsoft created a LNK file for the directory a file is opened from. Additionally, when a directory is created, Windows creates a LNK file for the directory created and for the created directories "parent" and "grandparent" directory. In addition to all the information LNK files record, LNK files also record the last time a file was opened.

Jump Lists — One of the newest artifacts to identify files opened by a user are "Jump Lists." Starting in Windows 7, Microsoft introduced two types of jump lists: "AutomaticDestinations" and "CustomDestinations." Automatic and Custom jump lists are created and stored in their respective directory in each user's home directory under the "AppData\ Roaming\ Microsoft\ Windows\Recent" directory. Each application can incorporate its own jump lists as a "mini-start" menu. AutomaticDestinations allow a user to quickly "jump" to or access files they recently or frequently used, usually by right-clicking the application in the Windows taskbar. CustomDestinations allow a user to pin recent tasks, such as opening a new browser window or create a new spreadsheet to the jump list.

Jump lists are essentially mega LNK files. Each jump list can record upwards of the last 1,000 files opened by each application. As jump lists are essentially compound LNK files, they contain all the same information as LNK files, such as when each file was opened, modified, accessed, and created; dates and times that the file was opened; the full directory path, volume name, and volume serial number from where the file was last opened; and the file size.

Most Recently Used (MRU) Registry Keys – As previously mentioned, the Windows Registry is a series of massive databases that track system configuration and user activity. There are several registry keys that track most recently used items. An analysis of these registry keys can help an analyst quickly identify files accessed. Every application developer has the option of creating registry keys specific to his

application configuration and user activity. Three of the most useful registry keys that track files accessed are "RecentDocs," "Microsoft Office FileMRU," and "OpenSavePIDMRU."

RecentDocs — The "RecentDocs" registry key tracks the name and order of the last 10 files opened for every file extension (e.g. .doc, .docx, .jpg, etc.). The registry organizes each of the last 10 files opened in sub keys named by the file extension. A sub key named "folder" is also created when the first folder is opened using the Windows Explorer. This sub key tracks the name of the last 30 folders opened. Each user has his own RecentDocs registry key located in his NTUSER.DAT registry hive under the "\Software\ Microsoft\ Windows\ Currentversion\ Explorer" registry key. The master RecentDocs key maintains a master list, organized in temporal order of the last 150 files or folders opened. By analyzing the order that particular files were opened, analysts have often been able to refute claims that a single type of file was opened by mistake. In one trade secret case, it was helpful for the analyst to show the pattern of files opened that all related to the same subject matter.

Applications Specific Most Recently Used (MRU) — With every Windows application, developers have the ability to create their own set of registry keys to track specific configuration and user activity for their application. If a specific application is used to commit or facilitate a crime or is otherwise significant to an investigation, it is often advantageous for the analyst to determine both if the application has its own set of registry keys and what actions those keys record. Two excellent examples are "Winzip," which records the name of the last several zip files created using the Microsoft Office suite of applications. Each application in the Office suite has its own set of "FileMRU" (most recently used files) that tracks most recent files used and when they were opened. Additionally, starting with Office version 365 and 2016, Microsoft Office tracks the "reading location" for each Word, PowerPoint, and Excel document opened and when each file was closed. Using this information, an analyst can determine not only what document was last opened and when it was closed, but also that the user had scrolled to and was on page 32 of the document when it was closed.

OpenSavePIDMRU — Windows has some basic dialog boxes that all programs can use when a user opens or saves a file. Some may have noticed that when saving files, a dropdown arrow in the file name dialog entry location appears. By clicking on the arrow, you will see several of the most recent file names you have saved for that application. These file names are saved as a part of the "OpenSavePIDMRU" registry key which is located under the "NTUSER.DAT \ Software\ Microsoft\ Windows\ CurrentVersion\ Explorer\ ComDlg32\ OpenSaveMRU" registry key. A record of the last 10 to 25 names of the last files opened or saved using the Windows Common Dialog Box are stored under sub keys based on file extension.

XI. Directory locations used

With the extensive storage capacity of standard hard drives today, it is often a challenge to find where users are storing information, particularly if they are trying to hide it. One technique digital investigative analysts can use to locate the directories from where a user is saving or accessing files is to analyze where the user has navigated, even when they did not open or save a file. We have already discussed several artifacts, such as LNK files, jump lists, and several MRU registry keys that document the full directory path where files were opened or saved. There is one additional artifact, the "LastVisitedPIDMRU," that, for each application, specifically tracks the last directory navigated to when opening or saving a file. Another artifact that also tracks the directories a user navigates, even when they do not open or save a file, is "ShellBags."

LastVisitedPIDMRU — The "LastVisitedPIDMRU" is a registry key located in the user's NTUSER.DAT registry hive in the "\Software\ Microsoft\ Windows\ CurrentVersion\ Explorer\ ComDIg32\" registry key. This key tracks the last directory a file is opened or saved in for each application. This is why when you go to open a document, the MS Word dialog box opens the directory in which you last opened or saved a word document. In a recent case, the analysis of the LastVisitedPIDMRU registry key revealed the user had last opened a Word document from a hidden truecrypted container that was previously mounted as "e:\HiddenTruecryptFolder." The data is stored in binary format, so conversion is necessary, but many registry forensic tools make this easy work.

ShellBags — Windows tracks user display preferences for the Windows Explorer in a registry key called "ShellBags," located in the "UserClass.dat" registry hive. Anytime a user changes the way files are displayed in the Windows Explorer, everything from what columns are visible to display mode (e.g., large icons, small icons, details list, etc.), the user's preferences are updated in ShellBags, and the recent navigation history is recorded. If you have ever changed a folder and returned to that folder to find your new preferences intact, then you have seen Shellbags in action.

Shellbags only records information about a directory for folders that have been opened and closed in Windows Explorer at least once. In other words, the simple existence of a directory in Shellbags is evidence the specific user account once visited that folder. Shellbags also records when that directory was first visited or last updated. Sometimes, Shellbags also records information regarding the files in the listed folders. An analyst can use ShellBag information to refute an individual's claims to have no knowledge about a directory with incriminating information inside. On more than one occasion, information from ShellBags has been used to prove someone using a specific user account had knowledge of an encrypted container because they had navigated there previously.

XII. Applications Used

Prefetch — A good first stop for identifying applications ran on a computer is the Windows "Prefetch" directory. Prefetching is the process of loading information from the hard drive into memory before it is needed. Prefetch began in Windows XP and is located in the "Windows\Prefetch" directory. Prior to Windows 10, a maximum of 134 prefetch files were stored at a time, as compared to 1,024 prefetch files stored with Windows 10. The prefetch file is designed to essentially be an audit log of all the files needed to execute a particular application. Any time an application is launched, the prefetch file monitors and creates a list of every file name and full directory path that is accessed during the initial execution of the application. Starting in Windows 8, prefetch also maintains the date and time the application was executed and the total number of times that application was run. Because users frequently open files (e.g., pictures, documents, spreadsheets, etc.) by double clicking on the file, analysts can often find the name and full path of several files opened by each application inside the prefetch file.

Imagine the value of identifying an otherwise covert application used to facilitate a crime that was launched from a USB drive or inside an encrypted directory. The application could even have been deleted from the computer, but a prefetch file will likely still exist showing when and how often the user executed the application. In one investigation, the defendant was identified using a portable Firefox browser on a thumb drive to surf the Internet, leaving no temporary Internet cache or other evidence on the office computer. Examination of the computer's prefetch files showed Firefox bring launched from a

USB drive, and when investigators obtained a warrant to search the portable thumb drive, they found it contained significant evidence of criminal activity and incriminating bookmarks.

UserAssist — The "UserAssist" registry key tracks all applications ran with a graphical user interface. The UserAssist registry key is frequently an artifact that complements the Windows Prefetch artifact previously discussed. Like Prefetch, the UserAssist key tracks applications ran and the number of times each application is executed; however, UserAssist also tracks the "focus count" and "focus time." Focus count records the number of times the application has come into primary focus of the Windows desktop. Focus time tracks the total time, down to the millisecond, each application was in primary focus on the Windows Desktop. This artifact has been useful when a defendant claims he had no knowledge that a specific application had run and suggests it must have been running in the background. With UserAssist, the analyst can tell exactly how often the application was run and how many hours, minutes, and seconds the application was the foremost active application on the desktop.

SRUM — As mentioned before, the System Resource Usage Monitor (SRUM) is an extensible storage engine (ESE) database located in the "c:\Windows\system32\sru" directory. Each hour, SRUM records every application running at that time and what user account is responsible for executing the application. Each hour, SRUM also records for each application the number of bytes written and read from disk and the bytes sent and received over the network. SRUM can be particularly useful in documenting the amount of data shared or downloaded by a particular peer-to-peer network program or, in a hacking case, how much data was exfiltrated out of the corporate network and when.

XIII. External USB Storage Devices

USB Storage Devices — Whether you are prosecuting theft of trade secrets, computer crime, or child pornography, tracking "thumb drives" (more accurately referred to as "USB storage devices") that have been connected to a single computer or across multiple systems can be crucial to an investigation.

To qualify for the Windows Logo Program "Designed for Windows," a USB device must have a unique serial number. This device serial number is burned into the firmware of the USB device and cannot be changed. Because this is unique to the USB device, it can be used to track when a specific USB device was inserted into multiple computer systems. If a device does not conform to the Windows Logo Program and has no unique device serial number, analysts can track such a USB device across multiple computers by using the "volume serial number." As long as the USB device is not reformatted, the volume serial number will remain the same across all Windows devices. The volume name of the device (e.g.,"Kingston Data Traveler" or "My Evil USB"), its device serial number, manufacturer, product identification (PID) number, and revision of a specific USB drive can be located in the "SYSTEM\CurrentControlSet\Enum\USBStor" registry key.

Starting in Windows 8, the first and last time a USB device was connected to a computer and the last time it was disconnected is recorded in the "\CurrentControlSet\ Enum\ USBStor\ Ven_Prod_Version\ Device_serial#\ Properties\ [83da6326-97a6-4088-9453-a1923f573b29}\" registry key. There are three sub-keys that have a 64bit hex timestamp in the key value that will identify these times: (a) first time USB device was inserted (Sub-Key: 0064); (b) last time USB device was inserted (Sub-Key: 0066); (c) last time USB device was unplugged (Sub-Key: 0067). Analysts can also identify the user account that was logged on when a device was connected by looking for the USB Device's Global Unique Identifier (GUID) found in the "SYSTEM\MountedDevices" registry key in the user's

"NTUSER.DAT\ Software\ Microsoft\ Windows\ CurrentVersion\ Explorer\ MountPoints2\" registry key.

Although not as definitive as the artifacts above, starting in Windows 8, an Event ID-20 log in the "Application and Services Logs\Microsoft\Windows\Audio\PlaybackManager" log file is created every time a USB device is connected to a system or removed without being properly ejected. Each event is associated with the audio tone heard when a device is connected or disconnected without going through the eject process. This event log does not identify a specific device, but an entry is created each time a device is attached or removed improperly and may be corroborative when combined with other artifacts, such as LNK files or jump lists.

XIV. Validating the Time is Correct

Analysts are often reluctant to commit to a timestamp of a file on a computer being accurate. Some will correctly point out that the time of the "Complementary metal–oxide–semiconductor" (CMOS /ˈsiːmos/) could have been changed prior to the operating system being booted. When the time an activity tool places on a computer is critical, there are two artifacts an analyst can check.

Event ID 1 and 4616 — The Windows operating system routinely reaches out to one of several time servers (e.g., time.windows.com, time.nist.gov) to synchronize the computer's clock time. Each instance the time is synchronized; the time of the computer is adjusted by milliseconds. An Event ID-4616 or ID-1 is created whenever the time on the computer is changed. The event log records when the time was changed, the previous time, and the new time. If a significant event occurred and it is critical to validate that the time of the event was recorded correctly on the computer, an analysis of event logs surrounding the event could be conducted to determine whether the computer was synchronized with the time server before and after the event at issue.

Event Log Record Sequence Numbers — All event logs have a hidden field about which most users and event administrators are unaware. For every event log, each event record is given a sequentially numbered "record number." If the time of an event is called into question by the suggestion that someone could have changed the date or time on the computer before the operating system started, an analyst could refute the claim by reviewing all of the event logs to show that no event record number was out of sequence. If someone changed the computer time forward or backward (typically in an attempt to establish an alibi), the event record numbers would clearly reveal this activity.

XV. Going back in time

Volume Shadow Copies — Beginning with Windows Vista, Microsoft started taking snapshots of almost every file on the system by default. Volume Shadow Copies are copies of files that have been modified since the last "system restore point" was made. Volume Shadow Copies have great potential to help law enforcement identify and document earlier versions of files or folders.

While Volume Shadow Copies are not as granular as saving every version of a saved document, they do provide significant information. In the user interface, the existence of previous versions of a document can be identified in the operating system by right clicking on the file or folder and then

selecting “restore previous versions.” The user has the option to open, copy, or restore, any of the previous versions. With previous versions, it may be possible to restore a shadow copy of a file that was deleted, even after the recycle bin has been emptied. The one caveat is that the analyst must know the original location of the file or folder. Testing has shown that if previous versions of a file are available and the file is moved to a new location on the hard drive, the list of previous versions will appear empty. This presents an interesting opportunity for forensic examiners to mount the volume shadow copy to their forensic workstation and examine previous versions of significant files or any specific digital artifacts.

XVI. Conclusion

There can be no doubt that significant challenges have recently arisen in the field formerly known as “computer forensics.” Law enforcement can help manage these challenges by rethinking the analyst’s role in the investigatory process. The prosecutor, agent, and analyst are all best served when collaborating and becoming an integral part of the investigation. Analysts can become more effective through a team-based, phased approach to digital investigative analysis. There is no longer any such thing as a “full forensic analysis,” so all analysis must be iterative. Once the analyst understands the changing needs of the prosecutor and agent, she is best positioned to identify the critical artifacts that will help establish the elements of the crime and respond to any likely defenses that may arise.

Prosecutors interested in these and other digital evidence issues and techniques can call CCIPS and the Cybercrime Lab, who are also available for consultation on digital investigative analysis and other technical investigative matters, by calling (202) 514-1026. Many other resources are available on our section's public website, www.cybercrime.gov.

ABOUT THE AUTHOR

❑ **Ovie Carroll** is the Director for the Department of Justice Cybercrime Lab at the Computer Crime and Intellectual Property Section (CCIPS) and has over 30 years of law enforcement experience. The Cybercrime Lab provides advanced digital investigative analysis, cybercrime investigative support, and other technical support to DOJ prosecutors as it applies to implementing the Department's national strategies in digital evidence, combating electronic penetrations, data thefts, and cyber attacks on critical information systems.

Mr. Carroll is also an adjunct professor with George Washington University for the Masters of Forensic Science program and is also a course author and certified instructor with the SANS Institute, where he teaches advanced computer forensics.

Mr. Carroll was also the Special Agent in Charge of the Computer Investigations and Operations Branch, Washington Field Office, Air Force Office of Special Investigations, where he was responsible for coordinating national level computer intrusions occurring within the United States Air Force. He has extensive field experience applying his training to a broad variety of investigations and operations. As a special agent with the AFOSI, Mr. Carroll has extensive field experience working general crimes, counterintelligence, and has conducted investigations into a variety of offenses, including murder, rape, fraud, bribery, theft, gangs, and narcotics.

Cultural Property

Judith Benderson
Attorney

I. Introduction

Cultural Property is a broad term used to cover art, artifacts, architecture, manuscripts, photographs, and almost anything created by humans or related to human activity. Under certain circumstances, it includes human remains. An ordinary cookie jar may become an item of value if it was owned by an historical figure or a celebrity. Pop artist Andy Warhol, for instance, collected cookie jars, and his ownership made those cookie jars disproportionately valuable. Former First Lady, the late Jacqueline Kennedy Onassis, owned a necklace of *fake* pearls which, after her death, was sold and then licensed for duplication, purely based on the fact that she owned and wore the original necklace.

Recent events in the Middle East have brought destruction to many architectural artifacts, such as the Temple of Bel in Palmyra in Syria. Simultaneously, however, the same people who destroyed much of the ancient city of Palmyra have also engaged in the looting of antiquities from Syria and Iraq to sell them and finance terrorist activities. An 81-year-old archaeologist, Khalil Al-Assad, was, in fact, beheaded for not revealing the location of many of Palmyra's most precious ancient objects.

But cultural property crime is much broader than looting of antiquities. It includes theft, forgery, fraud, and even tax crimes for art and artifacts.

There are many statutes, both in the United States and abroad, as well as international treaties and agreements that govern the sale and transfer of cultural property, encompasing import, export, and domestic. Much of this is addressed in an earlier United States Attorneys' Bulletin, *Cultural Property Law Enforcement (March 2016),* as well as in training for Assistant United States Attorneys and training by the FBI and Homeland Security.

This article, however, will address forensic issues, both scientific and non-scientific, that may come up in a cultural property case.

Cultural property investigations are likely to require consultation with experts in several areas. Considerations are authentication, identification, and valuation. To determine valuation, you must call upon professional appraisers, art dealers, or connoisseurs. Forensic scientists, curators, or academics might be used for authentication and identification. Appraisal societies can provide lists of appraisers with particular expertise, and there are some foundations established to study the work of a particular artist or artists, which, in the past, have been a source of authentication. However, they may or may not be helpful, as some of these foundations have stopped authenticating due to liability issues. Note that many academics and museum professionals, although willing to authenticate, are prohibited from valuing an object. Investigation of an object may be, at minimum, a two-step process, although it is not uncommon for both steps to occur simultaneously.

II. Authentication.

Is an object what it is presented as, or is it a forgery? How can that be established?

1) *Provenance* is the documentary history of a cultural object, including records of sale, importation, correspondence, authentication certifications, and the like. (This differs from "provenience," which is the site where a particular archaeological item was discovered.) Provenance used to have more significance in establishing celebrity ownership, thus making something more valuable, such as the Warhol-owned cookie jars mentioned above. Recently, it has been critical in helping determine if ownership actually existed and was legal. It is playing a serious role in the area of Holocaust Era art crime.

2) *Connoisseurship* is the discerning judgment of a subject matter expert, such as a museum professional or an academic, based on training and experience.

3) *Forensics* is the use of scientific tests and techniques to prove a relevant fact and is the subject of this Bulletin. Forensics can be used, for example, to determine if an object has circular saw marks indicating it may have been removed from its original location by a looter or if the old paint on a canvas was sanded down. Forgeries can sometimes be discovered if the materials used by the forger did not exist at the time of the creation of the original object. However, the best forgers may actually obtain old materials which existed at the time of the creation of similar objects and use them to create something entirely new in the hopes that it will escape scientific exposure.

There are arguments to be made as to which is the most important factor in a cultural property case, but it is likely that all three—provenance, connoisseurship, and forensics—may come into play.

When it comes to authenticating a work of fine art, consider whether the artist is living. If so, you may be able to interview that artist. Sometimes, especially with older work, the artist may not remember the piece in question or otherwise may have difficulty in conclusively authenticating it. This is not uncommon because some artists do not keep careful records of their work. It might come up where a piece has changed hands multiple times but it is unclear if it is the same work of art or part of a series, as titles may be inconsistent or have typographical errors in auction records. A prosecutor who lacks expertise in this field may not be aware that a particular art object is part of a series, so it is important to be certain both of the nature of a particular piece and that your research is not referring to a similar piece from the same artist. Not all artists are cooperative, but some are. Likewise, an authentication board might be a good source for an authentication witness, but as mentioned above, several authentication boards will no longer render opinions on authentication due to liability concerns. Two prominent examples are the Warhol Authentication Board and the Krasner-Pollock Foundation.

Another source to consider is the artist's *catalogue raisonne´*, if one exists. The New York Public Library defines "catalogue raisonne´" as a listing of all the known works of an artist either in a particular medium or all media. They may provide some or all of the following:

- Title and title variations
- Dimension/Size
- Date of the work
- Medium
- Current location/owner at time of publication

- Provenance (history of ownership)
- Exhibition history
- Condition of the work
- Bibliography/Literature that discusses the work
- Essay(s) on the artist
- Critical assessments and remarks
- Full description of the work
- Signatures, Inscriptions, and Monograms of the artist
- Reproduction of each work
- List of works attributed, lost, destroyed, and fakes
- Catalog number

Note that in the context of Native American cultural property, human remains are included under the Native American Graves Protection and Repatriation Act.

A. Provenance

Establishing provenance may require extensive research: bills of sale, gallery catalogues, museum records, newspaper reviews, or anything which can establish who may have owned an object and when. The longer and more extensive a provenance is, the more likely that authenticity may be established. Provenance is important in cases of looting, theft, and fraud.

B. Connoisseurship

Be aware that, as with many non-lawyers, connoisseurs may not provide an opinion in language that is preferred in the courtroom. A connoisseur witness might testify using language that comes across as vaguer than lawyers prefer. Rather than testifying that the work in question is a "fake," the connoisseur may say something like "it's not right." Conversely, a connoisseur may not state flatly that an object is authentic. However, there are ways to question such a connoisseur that include asking her to specify the basis for the opinion; the opinion might be stated in weak terms, but the connoisseur might have a convincing explanation in support of the conclusion. The connoisseur witness can also explain his or her extensive experience and years of training, and you can ask the witness about his or her level of certainty. If the witness is "100 percent" certain that the painting is "not right," that may be enough for your case.

C. Forensics

Forensics involve data with a scientific basis beyond observation and experience.

- Radiocarbon Dating: It is a scientific method used to date human or animal remains or any artifact containing organic material. All living organisms absorb carbon during their lives and stop upon their deaths. Scientists can estimate when the organism died based on the loss of Carbon 14.

- Stable Isotope Analysis: Forensic stable isotope analysis of human remains can provide important information in determining where a particular individual lived, because the ratio of Oxygen-18 to Oxygen-16 isotopes varies according to location. This analysis can even be used in studying teeth, as it helps identify where an individual lived during childhood.
- Satellite Data: Satellites are used to observe archeological sites, including looted areas. Satellite images can identify holes being dug in areas that could potentially contain archaeological resources, so law enforcement officers can examine the images for digging if looting is suspected. It is not possible to tie specific artifacts or human remains to a particular site through satellite data, but data can alert law enforcement to looting and potential trafficking. It is particularly useful in observing locations which might not be otherwise accessible, especially where there is military conflict.

Recently, in a non-looting example of using satellite data, a "space archaeologist" discovered a Viking settlement further west in Newfoundland than any previously known.

III. Object Identification

Object identification is important, as it should provide guidance and information as to what the object is. It should also be objective in that it does not pass any judgment on the item but describes it in the clearest possible way. This includes size, materials, markings, damage if any, etc., rather than using subjective criteria such as "sacred." Often a photograph is used with a measuring device next to it to establish size. Use of this sort of object identification may arise more often in cases involving artifacts. The J. Paul Getty Trust established standards for Object ID. OBJECT ID, http://archives.icom.museum/objectid/index.html (last visited Jan. 6, 2017). It provides much information about the why and how of object identification, and a checklist:

OBJECT ID CHECKLIST

PHOTOGRAPHS:

Photographs are important in identifying and recovering stolen objects. In addition to overall views, take close-ups of inscriptions, markings, and any damage or repairs. If possible, include a scale or object of known size in the image.

QUESTIONS:

- Type of object?
- What kind of object is it (e.g., painting, sculpture, clock, mask)?
- Materials & Techniques: What materials is the object made of (e.g., brass, wood, oil on canvas)?
- How was it made (e.g., carved, cast, etched)?
- Measurements: What is the size and/or weight of the object? Specify which unit of measurement is being used (e.g., cm., in.) and to which dimension the measurement refers (e.g., height, width, depth).
- Inscriptions & Markings: Are there any identifying markings, numbers, or inscriptions on the object (e.g., a signature, dedication, title, maker's marks, purity marks, property marks)?
- Distinguishing Features: Does the object have any physical characteristics that could help identify it (e.g., damage, repairs, or manufacturing defects)?

- Title: Does the object have a title by which it is known and might be identified (e.g., *The Scream*)?
- Subject: What is pictured or represented (e.g., landscape, battle, woman holding child)?
- Date or Period: When was the object made (e.g., 1893, early 17th century, Late Bronze Age)?
- Maker: Do you know who made the object? This may be the name of a known individual, a company, or a cultural group (e.g., tribe).

SHORT DESCRIPTION:

This can also include any additional information which helps to identify the object (e.g., color and shape of the object, where it was made).

KEEP SECURE:

Having documented the object, keep this information in a secure place.

OBJECT ID CHECKLIST, http://archives.icom.museum/objectid/checklist/english.pdf (last visited Jan. 6, 2017). Note that the date and maker may be the very subjects of your litigation.

IV. Valuation

Valuation may play a lesser role for purposes of government litigation. It is important in forfeiture cases to provide a base line value. For purposes of litigation, it is important to authenticate and identify as first steps, and then follow with valuation, just to be certain that the value is based upon the object being genuine.

Finally, your case will fall under Federal Rule of Evidence 702, which governs testimony by expert witnesses.

A witness who is qualified as an expert by knowledge, skill, experience, training, or education may testify in the form of an opinion or otherwise if:

(a) the expert's scientific, technical, or other specialized knowledge will help the trier of fact to understand the evidence or to determine a fact in issue;

(b) the testimony is based on sufficient facts or data;

(c) the testimony is the product of reliable principles and methods; and

(d) the expert has reliably applied the principles and methods to the facts of the case.

This is straightforward, but again, it is subject to some of the language vagaries that a connoisseur or dealer might use, so be sure the witness has a strong foundation. It is also critical to rule out any potential conflict of interest.

ABOUT THE AUTHOR

❑ **Judith Benderson** is a former attorney at the Office of Legal and Victim Programs in the Executive Office for United States Attorneys, where she dealt with cultural heritage issues and served as the Cultural Property Law Enforcement Coordinator. She has a Master of Fine Arts Degree in Painting and a Certificate in Appraisal Studies of Fine and Decorative Arts, both from George Washington University. She provided an appraisal in a forfeiture case, *U.S. v 18th Century Peruvian Oil on Canvas Painting of "Doble Trinidad"* and *17th Century Peruvian Oil on Canvas Painting of "Santa Rosa of Lima,"* 597 F.Supp.2d 618 (E.D. Va. 2009). As part of the Leadership Excellence and Achievement Program, she was assigned to the FBI Art Theft Program. She has taught frequently at the National Advocacy Center in Columbia, South Carolina. Most recently, she developed an online training program for Assistant United States Attorneys titled "The Prosecution of Cultural Property Crime," for the State Department.

The author wishes to thank Dave Hall, a former Assistant United States Attorney in the District of Delaware for 23 years and now a partner with Wiggin and Dana LLP. At DOJ, he was a special prosecutor with the FBI's Art Crime Team for eight years.

The author also wishes to thank Brad Meisel, a law student at Georgetown University School of Law, who provided research for this article, especially relating to the technical and scientific portions of it.

Forensic Accounting in Securities and Financial Fraud Prosecutions

Henry P. Van Dyck
Trial Attorney
Fraud Section
Criminal Division

L. Rush Atkinson
Trial Attorney
Securities & Financial Fraud Unit
Criminal Division

I. Introduction

Forensic accounting generally refers to accounting, auditing, and investigative techniques used to analyze and interpret complex or voluminous financial transactions. Forensic accounting may be used in all phases of the criminal case, including investigation, trial, and sentencing. During the investigative phase, forensic accountants may have to build and create databases and computer applications, manage bank statements and other financial records, trace funds and locate assets, provide opinions on the application of relevant accounting rules, and quantify the impact of a fraudulent act upon a company's financial statements. At trial, forensic accountants may testify about the results of their analyses, present summary exhibits and other visual aids, and provide an opinion about relevant accounting standards. At sentencing, forensic-accounting techniques may be used to estimate loss to investors, calculate restitution, and identify assets subject to forfeiture. Because forensic-accounting techniques have such a wide application to the criminal process, they have become an indispensable tool in the government's mission to combat securities and financial fraud.

II. Building the Case with Forensic Accounting

A. Choosing the Right Forensic-Accounting Professional

Fraud prosecutors who have no formal training in accounting principles may need to understand complex accounting issues during the investigation of a securities or financial fraud case. While most forensic accountants—whether employed directly by the government or as contractors—will have the investigative skills to trace funds or locate assets, consider whether your case may require additional specialized expertise. For example, during the investigation of a securities fraud case involving a public company, it may help to consult with a forensic accountant who also holds a license as a Certified Public Accountant, and thus, is qualified to explain relevant accounting standards and their potential application

to the investigative team. In other cases, such as an investigation into a potential Ponzi scheme involving a small group of perpetrators, nothing more may be required than a forensic accountant with the skills to build and manage a database containing bank records and other financial information and the ability to trace proceeds through multiple accounts. While most securities and financial fraud cases will benefit from using at least some forensic-accounting techniques, there will be cases where the specialized expertise of the forensic accountant also can be leveraged to advance the investigation.

B. Types of Analyses

In securities fraud prosecutions involving Ponzi schemes or misrepresentations in the sale of unregistered securities, forensic accounting techniques can build and maintain databases to hold the voluminous financial records gathered during the investigation, including bank statements, brokerage statements, and information provided by individual investors. As the database is populated with the evidence, forensic accountants can draw conclusions about the nature and extent of the scheme and resolve key questions in the case. The central issue in many Ponzi scheme cases is the extent to which the targets of the investigation used investor proceeds to pay off other investors, in violation of the terms of the investment. In very complex Ponzi schemes involving hundreds of accounts and multiple operating entities, forensic accountants may need to create a database with the financial records and collapse the transactions to show only inflows and outflows from the "system" that comprises the accounts linked to the scheme.

This technique was used by the government with success in *United States v. Timothy Durham et al.*, No. 1:11-CR-42 (S.D. Ind. 2012). In *Durham*, the defendants were charged with defrauding over 5,000 investors out of approximately $200 million after a financial services company collapsed with little or no assets available for recovery. The evidence at trial proved that the defendants had purchased an existing financial services company and stripped the company of its assets and liquidity through hundreds of related-party loans and lines of credit. Then, they used the proceeds from the loans to pay other investors, keep other failing businesses afloat, and sustain their lifestyle.

Because the defendants used a complex system of accounts to siphon investor proceeds through more than a hundred related businesses, the government relied upon forensic-accounting techniques to collapse all of the accounts controlled by the defendants so that the entire universe of cash flows into and out of the accounts was captured. This analysis showed that despite the defendants' glamorous lifestyle, the reality was that they were broke and their businesses were essentially insolvent. Nevertheless, at trial the defendants still argued that the value of their businesses was destroyed by the government's execution of a search warrant rather than by the fraud. The government was able to successfully counter that defense by relying upon the forensic accounting analysis to show that the only cash entering the defendants' system of accounts was investor proceeds. After a two-week trial, all defendants were convicted. Ultimately, the Chief Executive Officer of the collapsed financial services company received a 50-year sentence.

In contrast to securities fraud prosecutions involving the sale of unregistered notes, investigations into public companies often involve complex accounting issues. In many of these cases, the government will focus upon potential misrepresentations in the financial statements that the issuer has filed with the securities regulator, such as the Securities and Exchange Commission ("SEC"). The government often uses forensic accountants in these types of cases to help review the relevant papers from the company's outside auditors and establish what was known by the auditors about the transactions at that time. In addition, in a true accounting fraud case, the government also may ask the forensic accounting team to

provide an opinion on whether the financial statements were presented in accordance with relevant accounting principles, and to quantify the impact of the scheme upon the financial statements, in order to establish the materiality of the misrepresentations. *See United States v. Cuti*, 720 F.3d 453, 458 (2d Cir. 2013) (appropriate for the government to elicit testimony on materiality from "certified and experienced accountant[s] personally familiar with the accounting of the transactions at issue"); *United States v. Orr*, 692 F.3d 1079 (10th Cir. 2012) (noting government has broad discretion to prove materiality, including through posing hypothetical questions); *United States v. Ranney*, 719 F.2d 1183 (1st Cir. 1983). Forensic accountants who have specialized expertise in registered securities or Generally Accepted Accounting Principles can also assist in the investigation by explaining where the accounting records fit in with the scheme and the best way to examine the records, given the government's theory.

III. Presenting the Forensic Accounting Analysis at Trial: Summary Exhibits and Expert Testimony

A. Summary Exhibits

In complex securities and financial fraud prosecutions, the government often will rely upon summary financial charts to present the results of the forensic accounting analyses that took place during the investigation, introducing the evidence pursuant to Federal Rules of Evidence 1006 and 611(a). Rule 1006 permits the government to "use a summary, chart, or calculation to prove the content of voluminous writings, recordings, or photographs that cannot be conveniently examined in court," provided that the originals or duplicates are available for inspection and admissible. FED. R. EVID. 1006. "Such summaries are properly admissible when '(1) the charts fairly summarize voluminous trial evidence; (2) they assist the jury in understanding the testimony already introduced; and (3) the witness who prepared the charts is subject to cross-examination with all documents used to prepare the summary.'" *United States v. Hawkins*, 796 F.3d 843, 865 (8th Cir. 2015) (quoting *United States v. Green*, 428 F.3d 1131, 1134 (8th Cir. 2005)).

Often, the forensic accountant who conducted the analysis will introduce the exhibits and provide additional summary testimony. Such summary witness testimony about financial records is allowed in fraud cases under Federal Rule of Evidence 611(a), "which gives trial courts control over 'the mode [of] presenting evidence.'" *Hawkins*, 796 F.3d at 866 (quoting Fed. R. Evid. 611(a)). If the fraud case is sufficiently complex, it is also generally permissible to use a summary of witness testimony and/or trial exhibits to organize testimony and other evidence for the jury. *Id*. at 865. *See also United States v. Armstrong*, 619 F.3d 380, 385 (5th Cir. 2010) (affirming use of summary witness in insurance fraud trial); *United States v. Johnson*, 54 F.3d 1150, 1162 (4th Cir. 1995) (affirming use of a summary chart and summary witness in a drug conspiracy trial). When supported by testimony from a well-prepared witness, summary charts and graphs that explain the results of the forensic accounting analysis can be some of the government's most persuasive evidence in both proving the existence of a fraud scheme and showing how the scheme operated.

However, because the same point can be made through many different types of visual presentations, it also may be important to consider the visual impact of the summary exhibit and whether the point of the exhibit is likely to come across in a clear and concise manner. For example, where the

forensic accounting investigation has shown that the defendants were using investor proceeds for personal expenses, a single summary exhibit could focus upon just one of the defendant's extravagant purchases, with charts used by the forensic accountants to show that the purchase was paid for by investors. In other cases, it may be advantageous to present summary charts that show both specific examples of fraudulent transactions, as well as a global or high-level view of the scheme.

B. Summary v. Expert Testimony

A key consideration when presenting the results of the forensic accounting analysis at trial is whether the forensic accountant should testify as a lay witness or whether the analysis has crossed over into the realm of expert testimony, triggering additional notice and disclosure obligations under Federal Rule of Criminal Procedure 16 and Federal Rule of Evidence 702. Because forensic accounting is a discipline that constitutes "scientific, technical, or other specialized knowledge," FED. R. EVID. 702(a), the characterization of forensic accounting testimony as expert or non-expert may turn on the extent to which the results of the analysis is expressing an opinion or simply presenting the results of complex calculations.

The mere fact that a witness is an accountant and is testifying about financial statements does not mean the testimony is necessarily expert. For example, in *United States v. Georgiou*, 777 F.3d 125, 143(3d. Cir. 2015), (2015), the government offered the testimony of an SEC employee whose testimony involved "comparisons of stock quantities and prices" and "provided factual information and summaries of voluminous trading records that he had personally reviewed." *Id.* at 143–44. The testimony hewed mainly to "present[ing] testimony and accompanying charts concerning the manipulative trading activity charged in the indictment . . . and explain[ing] the relevance of his trading analysis to the other evidence presented in the case." *Id.* at 144 (internal quotation marks and alterations omitted). The Third Circuit held that this summary testimony of voluminous records was properly admitted as lay testimony. *Id.; cf. United States v. STABL, Inc.*, 800 F.3d 476, 487 (8th Cir. 2015) ("[M]ere tabulation does not require scientific, technical, or other specialized knowledge.").

Electing not to disclose a forensic accountant ahead of trial carries some risk that a court could later find his or her testimony to be expert and preclude the testimony as a sanction for violating Rule 16's expert-notice requirements. *See United States v. Hoffecker*, 530 F.3d 137, 184 (3d Cir. 2008) (holding where defendant provided notice three days before trial, it was "clear that the court did not abuse its discretion when it excluded [defendant's] expert witnesses as a sanction for violating Rule 16(b)(1)(C)"); *United States v. Day*, 524 F.3d 1361, 1371 (D.C. Cir. 2008) (holding it was proper to exclude expert witness testimony); *United States v. Petrie*, 302 F.3d 1280, 1288–89 (11th Cir. 2002) (same). If the government believes that an accountant's testimony is straddling the line between lay and expert testimony, early disclosures can avoid the potential loss of such important testimony.

IV. Sentencing and Loss Calculations

Forensic-accounting techniques also have a significant role to play in securities and financial fraud prosecutions during sentencing. One key driver in the Sentencing Guidelines for fraud cases is the amount and extent of loss suffered by victim-investors, which is calculated under Section 2B1.1 of the Sentencing Guidelines. In addition, the government must seek restitution on behalf of the victims, as required by the Mandatory Victims Restitution Act ("MVRA"), 18 U.S.C.A. § 3663A. In complex cases

involving hundreds or even thousands of investors, the government may use forensic-accounting techniques to quantify the loss for both sentencing and restitution purposes.

A. Loss Calculations

Importantly, while forensic accountants often are used to help calculate loss, the Sentencing Guidelines do not require absolute precision before the court can adopt a loss figure. Instead, "[t]he court need only make a reasonable estimate of the loss." *See* U.S. SENTENCING GUIDELINES MANUAL § 2B1.1 cmt. n.3(C) (U.S. SENTENCING COMM'N 2016); *see also United States v. Jackson*, 155 F.3d 942, 948 (8th Cir. 1998) ("In the case of fraud or theft, the loss need not be determined with precision. The court need only make a reasonable estimate of the loss, given the available information." (Internal citation and quotation marks omitted)). Loss can be the sum of different forms of loss, and the court is never bound to consider just one type of loss. For example, in a public securities fraud that involves the collapse of the company itself, the government may prove that the loss attributable to the fraud scheme includes both losses to shareholders as well as losses to insurers, whether private or quasi-public (such as the Federal Deposit Insurance Corporation). In *United States v. Shabudin*, No. 11-cr-00664-JSW-1 (NJV), 2014 U.S. Dist. LEXIS 50703(N.D. Cal. Apr. 8, 2014), a case concerning bank officers hiding losses from investors and regulators, the court ultimately found that the conspiracy caused the failure of the bank. For that reason, both loss and restitution were calculated to be over $900,000,000.

For public securities fraud, the United States Sentencing Commission has promulgated a special rule for quantifying actual loss in cases involving the fraudulent inflation or deflation in the value of a publicly traded security or commodity, which is codified in Application Note 3(F)(ix) of the Sentencing Guidelines. Under the Guidelines rule, last amended as of November 2015,

> In a case involving the fraudulent inflation . . . in the value of a publicly traded security or commodity, the court in determining loss may use any method that is appropriate and practicable under the circumstances. One such method the court may consider is a method under which the actual loss attributable to the change in value of the security or commodity is the amount determined by—(I) calculating the difference between the average price of the security or commodity during the period that the fraud occurred and the average price of the security or commodity during the 90-day period after the fraud was disclosed to the market, and (II) multiplying the difference in average price by the number of shares outstanding.

This method for calculating loss, also known as the "modified rescissory" method, was previously adopted by the Third and Eleventh Circuits. *See United States v. Brown*, 595 F.3d 498, 524 (3d Cir. 2010), (explaining use of "average selling price methodology"); *United States v. Snyder*, 291 F.3d 1291, 1296 (11th Cir. 2002) (calculating loss by taking difference between average price of stock of defendant's company during fraud and after disclosure of fraud to determine average loss per victim, multiplied by total number of victims). In most public securities fraud cases, the modified rescissory method will be the starting point of all loss calculations conducted by the forensic accountant because shareholder loss will constitute a significant, if not the majority of, loss. Until 2015, application note 3(F)(ix) in the U.S. Sentencing Guidelines made the modified rescissory method the presumptive calculation of shareholder loss. In 2015, however, the Sentencing Commission amended the note to make the modified rescissory

method a permissible but not compulsory way to calculate loss. While the method should be deemed a "reasonable estimate" of loss, some courts have required or favored a more complicated methodology to calculate shareholder loss.

In cases involving the fraudulent sale of unregistered securities that were held by individual investors, the loss calculations—while time consuming—may not require sophisticated accounting techniques. However, enlisting the assistance of a forensic accountant still may be the most reliable means to arrive at a reasonable loss estimate. Defendants in accounting and financial fraud cases, for example, often try to peg the loss calculation to the gain that they received (which can be more easily identified by looking just to the defendant's bank account or pay stubs). This argument directly contradicts the Guidelines, which provide that "the court shall use the gain that resulted from the offense as an alternative measure of loss *only* if there is a loss but it reasonably cannot be determined." U.S. SENTENCING GUIDELINES MANUAL § 2B1.1 cmt. n.3(B) (U.S. SENTENCING COMM'N 2016)) (emphasis added). Enlisting a forensic accountant to review the voluminous financial records will give the court a truer picture of the loss attributable to the defendant's scheme.

B. Restitution

The MVRA also states that a sentencing court "shall order . . . the defendant [to] make restitution to the victim of the offense." 18 U.S.C. § 3663A(a)(1) (2012 & Supp.); *see also United States v. Frazier*, 651 F.3d 899, 903 (8th Cir. 2011) (discussing the obligations to order restitution to identified victims in the amount of the victim's loss). The MVRA defines a victim as follows:

> a person directly and proximately harmed as a result of the commission of an offense for which restitution may be ordered including, in the case of an offense that involves as an element a scheme, conspiracy, or pattern of criminal activity, any person directly harmed by the defendant's conduct in the course of the scheme, conspiracy, or pattern.

18 U.S.C. §§ 3663(a)(2) (2012) and 3663A(a)(2) (2012 & Supp.). In many public securities fraud cases, the largest set of victims entitled to restitution are shareholders. Rather than just relying upon a cumulative measurement of loss, however, restitution in shareholder-loss cases often requires the government to specifically identify the shareholders during a particular time period—a task complicated by the fact that most individuals purchase stock through larger institutions such as their mutual-fund, brokerage firm, or investment advisor. When identifying victims with particularity is necessary, forensic accountants are critical to ensuring that individual victims are compensated. Using multiple data sources ranging from SEC data to filings in civil class-action lawsuits, accountants can successfully identify shareholder victims and their individual losses, albeit through a time-and resource-intensive project.

Given the time necessary to calculate individualized restitution, the government sometimes will consider asking the Court to defer the final entry of restitution until 90 days after sentencing pursuant to the Court's authority granted in 18 U.S.C. § 3664(d)(5) *See Dolan v. United States*, 560 U.S. 605, 624 (2010) (noting statutory authority to make "a final determination of the victims' losses" within 90 days of sentencing). This 90-day period after the pronouncement of sentencing can give forensic accountants time to identify additional victims. And in cases where the loss period was a matter of contention at sentencing, calculating restitution after sentencing also allows the accountants to frame restitution within the findings of the court as to when the fraud began and ended.

IV. Conclusion

Forensic accounting techniques are indispensable tools routinely used to support the government's mission to combat complex securities and financial fraud schemes. Whether the case involves a Ponzi scheme with just a few dozen investors or a complex accounting fraud at a public company, forensic accountants can help find assets, trace funds, apply and interpret accounting rules, build databases with bank statements and financial records, track cash inflows and outflows, calculate loss, and serve as a lay or expert witness at trial and sentencing.

ABOUT THE AUTHORS

❑ **Henry P. Van Dyck** is a Trial Attorney for the Fraud Section of the Criminal Division. Mr. Van Dyck has served as a prosecutor on successful cases such as *United States v. Lundstrom* and *United States v. Michael Baker and Michael Gluk*.

❑ **L. Rush Atkinson** is a Trial Attorney for the Securities & Financial Fraud Unit of the Criminal Division. Mr. Atkinson has been instrument of the prosecution of several high profile cases such as *United States v. Lundstrom.*

Investigation and Prosecution of Drone Cases: Emerging Issues for Prosecutors Confronting Unmanned Aircraft Systems

Gretchen C. F. Shappert
Assistant Director
Indian, Violent and Cyber Crime Staff
Office of Legal and Victim Programs
Executive Office for United States Attorneys

I. Introduction

Until recently, unmanned aircraft systems (UAS)—also known as "drones"—were novelty items with limited practical applicability and of little concern to most prosecutors. For many Americans, the first incident that demonstrated the potential for UAS operation to run afoul of federal law involved a recreational operator whose drone crashed onto the White House lawn on January 26, 2015. According to published news reports, a forensic analysis of the incident revealed that the drone operator was not in control of the drone when it crashed. No criminal charges were filed despite Federal Aviation Administration (FAA) regulations that prohibit the operation of unauthorized drones within the nation's capital regardless of the operator's intent. Spencer S. Hsu, *Man Whose Drone Crashed at White House Won't Be Charged; Fine Possible*, WASHINGTON POST, Mar. 18, 2015.

The dramatic proliferation of UAS and the consequences of rapidly advancing UAS technology cannot be overstated. Internationally, UAS are regulated by twelve countries and the European Union. Domestically, the number of registered UAS currently exceeds the number of registered manned aircraft. The FAA projects that sales of UAS intended for commercial use in the United States will triple from 600,000 in 2016 to 2.7 million in 2020. Ashley Halsey III, *Before Feared Spike in Drone Crashes, White House Sets New Rules*, WASHINGTON POST, June 21, 2016. In June 2016, the FAA announced the first operational rules for routine commercial use of small UAS (weighing less than 55 pounds), which became effective August 29, 2016. The new rules lifted previous restrictions that required UAS operators to have an FAA-issued pilot's license and a special waiver before flying UAS for commercial purposes. Brian Fung, *As of Today, It's Finally Legal to Fly Drones Commercially*, WASHINGTON POST, Aug. 29, 2016.

As the President observed in a February 2015 Presidential Memorandum, there is a wide spectrum of domestic users who are expecting to use UAS, "which may play a transformative role in fields as diverse as urban infrastructure management, farming, public safety, coastal security, military

training, search and rescue, and disaster response." Farmers use UAS to survey land, monitor water conservation, and study the health of crops. Kellen Browning, *Local Advocates Celebrate FAA's New Drone Regulations*, THE DAVIS ENTERPRISE, July 1, 2016. Real estate professionals use UAS to offer clients panoramic views of commercial and residential property. Lisa Conley, *The Sky's the Limit: FAA Approves Commercial Drone Use and Real Estate Industry Rejoices*, NAPLES NEWS, July 26, 2016. Companies such as Domino's Pizza and 7-11 have partnered with UAS operator Flirtey to deliver pizzas, Slurpees, and other products via drone. Christina Mulligan, *Domino's Announces a Pizza Drone Delivery Service*, INTERDRONE, Aug. 26, 2016. Amazon has created a pilot program dubbed "Amazon Prime Air" for drone delivery of merchandise. Farhad Manjoo, *Think Amazon's Drone Delivery Idea is a Gimmick? Think Again*, N.Y. TIMES, Aug. 10, 2016.

Law enforcement agencies have also begun to use UAS for investigative purposes. In England and Wales, more than a quarter of police departments are considering using drones to assist with criminal investigations. Victoria Ward, *Police to Use Drones to Aid Criminal Investigations*, TELEGRAPH, Jan. 5, 2016. In the United States, the Department of Justice issued guidance regarding the use of UAS by law enforcement components in investigations, and it is conducting tests to measure how well UAS can assist with accident reconstruction in 2017. Aliya Sternstein, *Justice Wants Drones to Try Reconstructing Car Crashes*, NEXTGOV, July 5, 2016. The recent FAA Extension, Safety, and Security Act of 2016 provides for UAS support in firefighting operations and mandates UAS collision research.

Although there are not yet any UAS-specific federal criminal statutes, a number of laws and regulations restrict or prohibit misuse of UAS by the public. Two charts (attached) list state and federal laws that may be relevant to UAS-related investigations and prosecutions. The following discussion offers background regarding some of the legal issues that may arise in cases involving UAS.

II. Drones and Criminal Law

A. Department of Justice Guidance on UAS

On February 15, 2015, the White House issued a presidential memorandum entitled, "Promoting Economic Competitiveness While Safeguarding Privacy, Civil Rights, and Civil Liberties in Domestic Use of Unmanned Aircraft Systems." Memorandum from President Barak Obama to The Heads of Executive Departments And Agencies (Feb. 15, 2015). On May 22, 2015, the Department of Justice issued agency-wide guidance on the use of UAS by its law enforcement agencies. DEPT. OF JUSTICE, POLICY GUIDANCE: DOMESTIC USE OF UNMANNED AIRCRAFT SYSTEMS (2015). The guidance notes that UAS have emerged as viable law enforcement tools to support kidnapping investigations, search and rescue operations, drug interdiction, and fugitive investigations, among other functions. The guidance reiterates, however, that deployment of UAS must be consistent with the U.S. Constitution and the laws, regulations, and policies that govern Department activities and operations, including those protecting privacy and civil liberties.

Under the DOJ guidance, for example, UAS may be used only in connection with properly authorized investigations and activities. Prior to use, Department personnel must assess the relative intrusiveness of UAS deployment, balanced against the particularized investigative need, taking into consideration factors such as whether the subject possesses a reasonable expectation of privacy relative to the proposed UAS use; the scope of the proposed use; the risk of disclosure to the subject; the seriousness of the crime or national security threat; the strength and significance of the information to be obtained; the

efficiency of method versus alternative means available; the amount of information already known about the subject; and the operational security needs of the investigation. To promote accountability, the DOJ guidance requires that approval for UAS use be granted at the Assistant Special Agent in Charge or equivalent level in the relevant field office, and by an executive level supervisor within the agency's aviation support unit or a designated executive level supervisor at the agency's headquarters. The DOJ guidance also requires consistent safeguards regarding data retention, annual privacy reviews by Senior Component Officials for Privacy, and annual reports to the Deputy Attorney General.

B. Constitutional Issues Surrounding Law Enforcement Deployment of UAS

Federal courts have not directly addressed the constitutionality of warrantless UAS surveillance during government investigations. However, several Supreme Court cases may support warrantless UAS surveillance under certain circumstances. *See Florida v. Riley*, 488 U.S. 445 (1989) (upholding the constitutionality of warrantless helicopter surveillance 400 feet above defendant's greenhouse); *California v. Ciraolo*, 476 U.S. 207 (1986) (upholding the constitutionality of warrantless airplane surveillance 1,000 feet above private property); *Dow Chemical Co. v. United States*, 476 U.S. 227 (1986) (EPA had statutory authority under the Clean Air Act to use aerial photography to perform "site inspection," and aerial photography of the chemical company's industrial complex was not a "search" for Fourth Amendment purposes). *But see United States v. Causby*, 328 U.S. 256 (1946) (holding that a compensable Fifth Amendment "taking" is cognizable where government flights invaded the "immediate reaches above" plaintiffs' land). Judicial decisions regarding the constitutionality of warrantless UAS surveillance are likely to be highly fact-specific, weighing expectations of privacy and the scope of the surveillance.

Notably, in *Riley*, Justice White's majority opinion recognized that warrantless surveillance of the defendant's property was constitutional in part because helicopters were available to the general public and not uncommon in the vicinity of the property. Therefore, the defendant had no reasonable expectation that a helicopter would be prohibited from viewing the details of his property observed by the police helicopter. *But see United States v. Cuevas-Sanchez*, 821 F.2d 248 (5th Cir. 1987) (placing a surveillance camera to record all of the activity in defendant's backyard was a "search," but a search warrant authorizing video surveillance for 30 days did not violate the Fourth Amendment). In the UAS context, hundreds of civilian UAS are available for retail for prices starting at below $20.00, and the FAA estimates that total drone sales will grow from 2.5 million this year to 7 million in 2020. Hence, the expectation that a drone may view details of real property today may be comparable to the expectation that a helicopter may do so.

However, using UAS to collect information about the intimate details of a residence or its occupants is likely to raise constitutional issues comparable to those addressed in *Kyllo v. United States*, 533 U.S. 27 (2001) (holding that the warrantless use of a thermal imaging device not available to the general public that revealed intimate details of the home was unconstitutional). Federal courts could also analogize drone surveillance to the warrantless installation of a GPS tracking device in a suspect's vehicle, which the Supreme Court decided was unconstitutional in *United States v. Jones*, 132 S. Ct. 945 (2012). If warrantless UAS surveillance is challenged on constitutional grounds in a federal criminal case, prosecutors may consider producing technical experts to explain how drone technology, operations, and retail make UAS more analogous to the aircraft in *Riley* and *Ciraolo* than to the thermal imaging device in

Kyllo or the GPS tracking device in *Jones*. Of course, obtaining a search warrant prior to UAS surveillance will help to ameliorate such challenges.

One recent example of an oblique constitutional challenge involved a father and son in Connecticut, Bret and Austin Haughwout, who challenged the FAA's use of administrative subpoenas requiring disclosure of information about the use of weaponized drones in YouTube videos recorded in their backyard. Amanda Pinney, *Father, son fight FAA over gun-firing, flame-throwing drones*, THE DAILY DOT, (July 5, 2016). One video shows a drone equipped with a handgun firing rounds. A second video shows a drone equipped with a flamethrower igniting a spit-roasting Thanksgiving turkey. The Haughwouts challenged the FAA's authority to regulate recreational drone use, contending that the FAA did not have good faith or a legitimate purpose for its investigation because UAS are not properly subject to regulation as "aircraft" under the FAA's statute. *See Huerta v. Haughwout*, 3:16-cv-358, slip op. at 2 (D. Conn. July 18, 2016).

The district court was unpersuaded by the Haughwouts' arguments. The court noted that it seemed clear "that Congress intends for the FAA to regulate at least *some* drones owned by individuals," citing the FAA Modernization and Reform Act of 2012, P.L. 112-95 §§ 331–336 (codified at 49 U.S.C. § 40101 note) and regulatory interpretations of "aircraft" as encompassing "unmanned aircraft." *See Huerta v. Pirker*, 2014 WL 8095629 (N.T.S.B. Nov. 17, 2014). But the district court also noted the existence of "substantial questions about the scope of the FAA's regulatory enforcement authority," including whether "Congress intends—or could constitutionally intend—to regulate all that is airborne on one's own property and that poses no plausible threat to or substantial effect on air transport or interstate commerce in general." *Huerta*, 3:16-cv-358, slip op. at 4.

C. UAS and Federal Criminal Prosecutions

Public use of UAS may implicate a number of criminal laws. For example, the FAA has designated the 15-mile radius surrounding Ronald Reagan National Airport (which includes all of Washington, D.C.) as a "No Drone Zone," as part of the Special Flight Rules Area (SFRA) for the National Capital Region (NCR). FED. AVAITION ADMIN., NO DRONE ZONE (2016). Special events such as the Super Bowl and the Republican and Democratic national conventions have also received temporary "No Drone Zone" designations. FED. AVAITION ADMIN., NEW FAA VIDEO EXPLAINS THAT THE SUPER BOWL IS A NO DRONE ZONE (2016). In October 2015 testimony before the FAA, Deputy Administrator Michael Whitaker stated that the FAA "will work with our local law enforcement partners to prosecute" those who endanger other aircraft or people and property on the ground. *Ensuring Aviation Safety in the Era of Unmanned Aircraft Systems:* Hearing before the Aviation Subcomm. of the H. Transportation and Infrastructure Committee, 161st Cong. Rec. D1071-01 (2015) (statement of Dep. Adm' Michael G. Whitaker).

As noted above, the chart attached to this article lists several federal criminal statutes that may be relevant to such federal criminal prosecutions.

In one of the first federal drone prosecutions, the U.S. Attorney's Office for the District of Hawaii prosecuted a defendant for violating lawful orders of a U.S. park ranger, including an order to refrain from flying a drone over a crowd gathered to view the Halema'uma'u crater in Hawaii Volcanoes National Park. Press Release, Dept. of Justice, U.S. Attorney's Ofc. Dist. of Haw., Hilo Man Convicted Of Disobeying Park Ranger (Feb. 12, 2016). *See also United States v. Sanders*, 1:15-cr-00558 (D. Haw. 2016). Although the defendant in *Sanders* was convicted only of disobeying one of the other orders issued

by the Park Ranger, the case is notable for underscoring some of the challenges associated with drone-related prosecutions. For instance, the applicability of federal regulations governing aircraft in federal parks has been questioned because they define "aircraft" as "a device that is used or intended to be used for human flight in the air, including powerless flight," *see* 36 C.F.R. § 1.4 (2017), or prohibit air delivery with provisions that restrict "[d]elivering or retrieving a person or object ... by other airborne means . . ," *see* 36 C.F.R. § 2.17(a)(3) (2017); *see also* Gregory S. Neal, *Yosemite Looks to Ban Drones by Relying on an Absurd Legal Argument*, FORBES, May 3, 2014. In *Sanders*, federal prosecutors also alleged a violation of the Hawaii Volcanoes National Park Superintendent's Compendium of 2015, which specifically prohibits the use of "unmanned aircrafts." Prosecutors should consider this example in determining applicable sources of law in drone-related investigations.

Other federal drone prosecutions have involved drug smuggling. In what is believed to be the first case of its kind, two California residents recently pleaded guilty to smuggling 28 pounds of heroin into the United States from Mexico using drones. Press Release, Dept. of Justice, U.S. Attorney's Ofc. S. Dist. of Cal., International Smuggling by Drones Nets 28 Pounds of Heroin (Aug. 12, 2015). Another case that originated in California involved an unsuccessful attempt to deliver a cell phone to an incarcerated person in a federal prison. Press Release, Dept. of Justice, U.S. Attorney's Ofc. C. Dist. of Cal., Federal Inmate who Orchestrated Stolen Check Scheme from Prison Sentenced to Another 9+ Years in Multi-Million Dollar Fraud Case (Feb. 11, 2016). As recently as October 2016, the media has reported on the increasing use of drones to smuggle contraband, including heroin, marijuana, pornography, and cell phones, into prisons. Michael S. Rosenwald, "Prisons Try to Stop Drones From Delivering Drugs, Porn and Cellphones to Inmates," WASH. POST, Oct.13, 2016. In July 2015, a drone dropped a quarter ounce of heroin, two ounces of marijuana, and more than five ounces of tobacco into the yard of an Ohio prison immediately before a fight broke out.

The versatility and sophistication of drone technology is also of interest to crime syndicates and foreign countries. Several recent cases involving drones have implicated the Arms Export Control Act (AECA), 22 U.S.C. §§ 2751–2799, which authorizes the President to control the export of defense articles and services of the United States, and the International Traffic in Arms Regulations (ITAR), 22 C.F.R. § 120 *et seq*. On February 17, 2015, the State Department issued the U.S. Export Policy for Military Unmanned Aerial Systems, which restricts the international sale of "U.S.-origin military and commercial UAS." Press Release, Bureau of Public Affairs, U.S. Export Policy for Military Unmanned Aerial Systems (Feb. 17, 2015).

One of the first AECA prosecutions involving UAS was brought against two Taiwan nationals in the District of New Jersey in 2014. Press Release, Dept. of Justice, U.S. Attorney's Ofc. Dist. of N.J., Two Taiwan Nationals Admit International Drug Trafficking, Attempting To Export United States Military Drone Technology To People's Republic Of China (Sept. 22, 2014). Hui Shen Shen and Huan Ling Chang approached undercover FBI agents in September 2011 and inquired about obtaining highly sensitive military drone technology restricted from export. The co-conspirators made arrangements to photograph the military drones and made plans for shipping the drones outside of the United States. In exchange for the drones, they arranged for a delivery of a sample of crystal methamphetamine and the subsequent shipment of a kilogram of the drug. *See* United States v. Shen, 2:14-cr-549 (D. N.J. Jan. 2015); United States v. Chang, 2:14-cr-548 (D. N.J. Jan. 2015).

Another relevant AECA prosecution involved a California woman who was convicted at trial on charges involving a scheme to export, among other things, a "General Atomics MQ-9 Reaper/Predator B Unmanned Aerial Vehicle, capable of firing Hellfire Missiles." *See United States v. Man*, 0:14-cr-60195 (S.D. Fla. Aug. 2016). Wenxia Man was sentenced to 50 months in prison for conspiring to export and cause the export of fighter jet engines, UAS, and related technical data to the People's Republic of China.

D. Possible Future Scenarios

Future scenarios may encompass all sorts of activities involving UAS, including circumstances involving UAS operators who lose control of "runaway" or "rogue" drones, which can create nuisances or even harm members of the public, to graffiti artists using UAS to deface tall billboards. Craig Whitlock, *Rogue Drones a Growing Nuisance Across the U.S.*, WASHINGTON POST, Aug. 10, 2015; Amber Sutherland and Natalie O'Neill, *Graffiti 'Artist' Uses Drone to Deface Kendall Jenner ad*, N.Y. POST, May 1, 2015.

One area of special concern is UAS interference with important government operations, such as wildland firefighting. Firefighters battling forest fires in California recently have complained that UAS intrusions into fire scenes more than doubled from 2014 to 2015. Rogue UAS operating near a fire scene may negatively impact the ability of firefighters to maneuver. In July 2016, for example, firefighters battling the Sand Fire in Southern California were forced to suspend aerial firefighting operations for about 30 minutes after an unauthorized UAS entered air space temporarily restricted by the FAA due to the active wildfire. Jeff Daniels, *As Sand Fire Rages, Feds Turn Up Heat in Fight Against Drones Interfering in Wildfires*, CNBC, July 26, 2016.

UAS facilitated acts of terror are also a possibility. The Haughwouts in Connecticut have demonstrated that UAS can be armed with harmful payloads, such as guns or flamethrowers. In 2015, the BBC reported that a man protesting the Japanese government's nuclear energy policy flew a UAS equipped with a small camera and radioactive material onto the roof of the Japanese prime minister's office. *Japan radioactive drone: Tokyo police arrest man*, BBC, Apr. 25, 2015. Although no one was hurt, the episode raised security concerns about extremists using UAS to carry out attacks. Indeed, as recently as October 2016, the New York Times reported that ISIS has employed so-called "exploding drones" against enemy forces. Michael S. Schmidt & Eric Schmitt, *Pentagon Confronts a New Threat from ISIS: Exploding Drones*, N.Y. TIMES, Oct.11, 2016.

Prosecutors interested in learning more about some of the unique legal challenges posed by prosecutions of UAS related conduct should contact the Department of Justice's Criminal Division.

III. The FAA and UAS

A. FAA's New Operational Rules for UAS

Small commercial UAS used for business purposes must comply with the new UAS rules contained in Part 107, any applicable Section 333 grants of exemption, and airworthiness registration requirements for the UAS. FED. AVIATION ADMIN., UNMANNED AIRCRAFT SYSTEMS (UAS) FREQUENTLY ASKED QUESTIONS/HELP (2016). Provisions of the rule, Part 107, provide for commercial use of small UAS weighing less than 55 pounds (including any payload, such as a camera) when operating in class G airspace without a written waiver. FED. AVIATION ADMIN. AIRSPACE CLASSIFICATION (2016).

Under these regulations, drones can fly only up to an altitude of 400 feet, with an airspeed of up to 100 miles per hour. Commercial drone pilots must hold either a remote pilot airman certificate with a small UAS rating or be under the direct supervision of someone who holds a remote pilot certificate (remote pilot in command). Flight must be conducted within the visual line of sight of the pilot and not from a moving vehicle or aircraft. Currently no drone is authorized to operate over any person not directly participating in the operation. Many restrictions are waivable if the applicant demonstrates that the operation can be conducted safely under the terms of the waiver. Media companies, for example, may request to fly over people if they have complied with the Part 107 waiver process. Persons seeking exemptions must demonstrate sufficient mitigation to ensure public safety. FED. AVIATION ADMIN., UNMANNED AIRCRAFT SYSTEMS (UAS) FREQUENTLY ASKED QUESTIONS/HELP (2016).

Recreational UAS users or hobbyists have two ways to operate in the national airspace system in accordance with FAA regulations. The first option is compliance with Congress's "Special Rule for Model Aircraft" included in section 336 of the FAA Modernization and Reform Act of 2012, which requires that the UAS only be used for hobby or recreational purposes; that the operator follow a community-based set of safety guidelines; that the UAS is operated only within visual line-of-sight; that the drone gives way to other aircraft; that the UAS operator gives notice to the airport and air traffic controller, if one is present, when operating a UAS within five miles of an airport; that the UAS weigh no more than 55 pounds, unless certified by the community-based organization; and the UAS is registered. H.R. REP. NO. 112-381 at 336 (2012). The second option requires the recreational UAS operator to comply with the FAA's Part 107 rules described above in order to obtain a remote pilot certificate or operate under the direct supervision of someone who holds a certificate, and to register the drone at "Register my UAS." FED. AVIATION ADMIN., WELCOME TO THE SMALL UNMANNED AIRCRAFT SYSTEM (sUAS) REGISTRATION SERVICE, (last visited Dec. 13, 2016) The FAA has also developed a model application called B4UFLY. FED. AVIATION ADMIN., UNMANNED AIRCRAFT SYSTEMS (UAS) REGULATIONS & POLICIES, (2016). Additional guidance is available at "Where to Fly." FED. AVIATION ADMIN., WHERE TO FLY (2016).

There are significant civil and criminal penalties for non-compliance with FAA regulations. FED. AVIATION ADMIN., UNMANNED AIRCRAFT SYSTEMS (UAS) REGULATIONS & POLICIES (2016) In October of 2015, the FAA announced that it was seeking a $1.9 million civil penalty against Chicago-based SkyPan International for allegedly conducting 65 UAS flights over New York and Chicago during a 33-month period. Press Release, Fed. Aviation Admin., FAA Proposes $1.9 Million Civil Penalty Against SkyPan International for Allegedly Unauthorized Unmanned Aircraft Operations (Oct. 6, 2015). Failure to register a UAS can result in civil penalties up to $27,000 and criminal penalties of up to $250,000 and/or imprisonment up to 3 years. Title 49 of the United States Code provides criminal penalties for failure to comply with UAS registration requirements, operation in national defense airspace, interference with air navigation, transporting hazardous materials, and refusing to comply with a Department of Transportation subpoena. 49 U.S.C.A. §§ 46306-46308, 43612-4313 (2016).

B. The FAA and Forensic Issues Associated with UAS

The FAA's safety mandate under 49 U.S.C. § 40103 requires that it regulate aircraft operations. It is possible that the FAA may take enforcement actions against persons operating UAS in a manner that endangers public safety. However, as noted by the district court in *Huerta v. Haughwout*, there is at least

some lingering doubt about the scope of the FAA's enforcement authority, and prosecutors will have to navigate with care the complex issues implicated by this ambiguity.

Federal, state, and local law enforcement agencies are often in the best position to detect, investigate, and pursue the initial enforcement actions when UAS use involves criminal activity. Because UAS operations implicate the FAA's safety mandate and unique aviation-related expertise, law enforcement officers and prosecutors are strongly encouraged to contact the FAA in any situation where UAS are suspected or identified as involved in criminal activity. To assist law enforcement in that process, the FAA maintains Regional Operation Centers (ROC) located around the country and staffed 24 hours a day with access to trained FAA personnel who are available to assist law enforcement when there has been a drone incident, accident, or other matter requiring FAA assistance. The FAA Law Enforcement Assistance Program (LEAP) also provides FAA Special Agents to assist with the investigation. FED. AVIATION ADMIN., LAW ENFORCEMENT ASSISTANCE PROGRAM (LEAP), (2016). All of these resources are available in the FAA's Law Enforcement Guidance for Suspected Unauthorized UAS Operations. FED. AVIATION ADMIN., LAW ENFORCEMENT ENGAGEMENT WITH SUSPECTED UNAUTHORIZED UAS OPERATIONS, (2016).

UAS also implicate unique evidentiary issues, which is why agents and prosecutors should consider engaging the FAA early in any investigation. UAS command-and-control mechanisms vary widely, and they continue to change as technology increases in sophistication. Some UAS may be operated by the same person with multiple types of controllers, and other UAS may be operated by two people at the same time. Hence, the investigation of drone activity requires that prosecutors and agents assess who actually exercised control over the drone and which laws or regulations are implicated in a given situation. For example, the FAA's operational rules require that a pilot-in-command (PIC) be at least 16 years old and possess a remote pilot airman certificate with a small UAS rating. An individual under the age of 16 or an individual without a remote pilot airman certification could also operate a drone when acting under the direct supervision of a person who holds such a certificate. The applicability of operational rules to a particular law enforcement investigation should be discussed with the FAA.

UAS may be comprised of several components: a platform, which includes the vehicle's frame; navigation systems (accelerometers, gyroscopes, magnetometers, airspeed sensors, and/or GPS trackers); communications systems; and payloads (e.g. sensors, optics, cargo). Most UAS record telemetry in both the unmanned aerial vehicle (UAV) and the ground control device (GCS), and a particular UAV can usually be linked to a specific GCS by comparing the UAV telemetry with the GCS telemetry. Telemetry may include GPS information (latitude, longitude, and time) as well as aircraft status and commands. However, there are no industry-wide standards on UAS telemetry, and telemetry can be deliberately altered or deleted. For all of these reasons, agents and investigators are encouraged, where possible, to collect the UAV, any GCS, and any other component of the UAS as quickly as possible after a drone incident in order to prevent alteration or tampering. Analysis of this evidence may be facilitated by FAA personnel or the UAS manufacturer.

Physical evidence that should be considered for collection in a drone investigation may include, but is not limited to, fingerprints, DNA, toolmark evidence, platform components, and payload. This physical evidence may help tie a UAS to one or more UAS operators. Digital evidence—including the UAS's sensory data storage and instructional coding—may help investigators and prosecutors determine the intent of the UAS operators.

One portion of the digital evidence that should be analyzed whenever possible is the pre-flight procedures. Careful review of the operator's pre-flight procedures and compliance with those procedures may help identify why a drone incident occurred. For example, if an operator does not properly set a "Return-to-Home" point, or does not wait for GPS to engage before take-off, a UAS could travel in an unexpected direction. For all of these reasons, coordination with FAA regulatory personnel in the LEAP, and consultation with UAS experts at the FAA or in private industry could be essential to the success of a UAS-related investigation or prosecution. LEAP assistance can be obtained via e-mail, Janet.Riffe@faa.gov.

The FBI has also developed resources to address UAS-related issues. Legal issues can be addressed to the FBI's Operational Technology Unit in the Office of the General Counsel. For technical assistance, prosecutors and agents should contact FBI's Operational Technology Division, TTA Operations & Development Unit.

IV. Conclusion

Investigating and prosecuting criminal cases that involve UAS may require forensic evidence and expert testimony to explain UAS technology and the nexus between the alleged operator and the offending unmanned aircraft. Does the particular device in question meet the statutory definition of an aircraft? Can the government demonstrate that the device was operated by the defendant?

Depending upon the charges in the Bill of Indictment, expert testimony may also be required to demonstrate the UAS's speed, height above the ground, proximity to national defense airspace, and/or interference with air navigation. Were the drone's activities covered by a Rule 333 exemption or FAA Part 107? Was the drone subject to commercial or recreational regulations? These are only a few of the issues that prosecutors will need to address as a new fleet of smaller, more sophisticated, and more discreet unmanned aircraft begin to fill the skies.

ABOUT THE AUTHOR

❑ **Gretchen C. F. Shappert** is the Assistant Director for the Indian, Violent and Cyber Crime Staff at the Executive Office for U.S. Attorneys. Ms. Shappert served as the U.S. Attorney for the Western District of North Carolina from 2004 to 2009. She was also an Assistant U.S. Attorney from 1990 to 2004 and specialized in violent crime and outlaw motorcycle gang prosecutions.

The author wishes to thank Victor W. Weedn, Senior Forensic Advisor to the Deputy Attorney General; Sean M. Douglass and Daniele Arad-Neeman, Office of Legal Policy; Cyrus Roohi, Senior Technical Advisor, FAA UAS Integration Office; Dean Griffith, UAS Regulatory Policy & Outreach Team Lead, FAA Office of the General Counsel; and most especially, Bradford Meisel, second-year law student, Georgetown University School of Law, and extraordinary summer intern at EOUSA.

FEDERAL DRONE CHART

Statute	Date Enacted	Penalty
18 U.S.C.A. § 32 Destruction of aircraft or aircraft facilities	July 14, 1956 Amended October 12, 1984	Fine and up to twenty years' imprisonment or both; if death results, shall be subject to the death penalty or to life imprisonment.
18 U.S.C.A. § 1361 Injuring Federal Property	October 11, 1996	If the damage or attempted damage to such property exceeds the sum of $1,000, by a fine under this title or imprisonment for not more than ten years, or both; if the damage or attempted damage to such property does not exceed the sum of $1,000, by a fine under this title or by imprisonment for not more than one year, or both.
18 U.S.C.A. § 1362 Injuring Communication Lines, Stations, or Systems	October 26, 2001	Fine, up to 10 years imprisonment, or both.
18 U.S.C.A. § 1363 Injuring Buildings of Property Within Special Maritime and Territorial Jurisdiction	October 26, 2001	Fine, up to 10 years imprisonment, or both.
18 U.S.C.A. § 1369 Destruction of Veterans' Memorials	May 29, 2003	Fine, up to 10 years imprisonment, or both.
18 U.S.C.A. § 1801 Video Voyeurism in Special Maritime and Territorial Jurisdiction	December 23, 2004	Fine, up to 1 year imprisonment, or both.
18 U.S.C.A. § 2261A Stalking	October 1, 2013	Imprisonment (1) for life or any term of years, if death of the victim results; (2) for not more than 20 years if permanent disfigurement or life threatening bodily injury to the victim results; (3) for not more than 10 years, if serious bodily injury to the victim results or if the offender uses a dangerous weapon during the offense; (4) as provided for the applicable conduct under chapter 109A if the offense would constitute an offense under chapter 109A (without regard to

		whether the offense was committed in the special maritime and territorial jurisdiction of the United States or in a Federal prison); and (5) for not more than 5 years, in any other case, or both fined and imprisoned. (6) Whoever commits the crime of stalking in violation of a temporary or permanent civil or criminal injunction, restraining order, no-contact order, or other order described in section 2266 of title 18, United States Code, shall be punished by imprisonment for not less than 1 year.
18 U.S.C.A. § 1465 Production and Transportation of Obscene Matters for Sale or Distribution	June 27, 2006	Fine, up to 5 years imprisonment, or both.
18 U.S.C.A. § 1466A Obscene Visual Representation of the Sexual Abuse of Children	April 30, 2003	Fine, up to 10 years imprisonment (up to 20 years if it involves minors under 12 years of age) or both.
18 U.S.C.A. § 1751 Presidential and Presidential Staff Assassination	August 28, 1965	Death or imprisonment for life
18 U.S.C.A. § 351 Congressional, Cabinet, and Supreme Court Assassination, Kidnapping, and Assault	January 3, 2012	Death or imprisonment for life.
18 U.S.C.A. § 1791 Providing of Possessing Contraband in Prison	August 10, 2010	(b) Punishment.--The punishment for an offense under this section is a fine under this title or-- (1) imprisonment for not more than 20 years, or both, if the object is specified in subsection (d)(1)(C) of this section; (2) imprisonment for not more than 10 years, or both, if the object is specified in subsection (d)(1)(A) of this section; (3) imprisonment for not more than 5 years, or both, if the object is specified in subsection (d)(1)(B) of this section; (4) imprisonment for not more than one year, or both, if the object is specified in subsection (d)(1)(D), (d)(1)(E), or (d)(1)(F) of this section; and (5) imprisonment for not more than 6 months, or both, if the object is specified in subsection (d)(1)(G) of this section.

		(c) Consecutive punishment required in certain cases.--Any punishment imposed under subsection (b) for a violation of this section involving a controlled substance shall be consecutive to any other sentence imposed by any court for an offense involving such a controlled substance. Any punishment imposed under subsection (b) for a violation of this section by an inmate of a prison shall be consecutive to the sentence being served by such inmate at the time the inmate commits such violation.
18 U.S.C.A. § 793 Gathering, Transmitting, or Losing Defense Information	October 11, 1996	Fine, up to 10 years imprisonment, or both.
18 U.S.C.A. § 794 Gathering or Delivering Defense Information to Aid Foreign Government	October 11, 1996	Death or imprisonment for any term of years or for life.
18 U.S.C.A. § 795 Photographing and Sketching Defense Installations	June 25, 1948	Fine, up to 1 year imprisonment, or both.
18 U.S.C.A. § 796 Use of Aircraft for Photographing Defense Installations	June 25, 1948	Fine, up to 1 year imprisonment, or both.
18 U.S.C.A. § 47 Use of Aircraft or Motor Vehicles to Hunt Certain Wild Horses or Burros	September 8, 1959	Fine, up to 6 months imprisonment, or both.
18 U.S.C.A. § 48 Production of Animal Crush Videos	December 9, 2010	Fine, up to 7 years imprisonment, or both.
18 U.S.C.A. § 41 Hunting, Fishing, Trapping; Disturbance or Injury on Wildlife Refuges	June 25, 1948	Fine, up to 6 months imprisonment, or both.
18 U.S.C.A. § 2342 Trafficking in Contraband Cigarettes and Smokeless Tobacco	March 9, 2006	(a) Whoever knowingly violates section 2342(a) of this title shall be fined under this title or imprisoned not more than five years, or both. (b) Whoever knowingly violates any rule or regulation promulgated under section 2343(a) or 2346 of this title or violates section 2342(b) of this title shall be fined under this title or imprisoned not more than three years, or both.
18 U.S.C.A. § 1864 Hazardous or Injurious Devices on Federal Lands	April 26, 1996	(b) An individual who violates subsection (a) shall--

		(1) if death of an individual results, be fined under this title or imprisoned for any term of years or for life, or both; (2) if serious bodily injury to any individual results, be fined under this title or imprisoned for not more than 40 years, or both; (3) if bodily injury to any individual results, be fined under this title or imprisoned for not more than 20 years, or both; (4) if damage to the property of any individual results or if avoidance costs have been incurred exceeding $10,000, in the aggregate, be fined under this title or imprisoned for not more than 20 years, or both; and (5) in any other case, be fined under this title or imprisoned for not more than one year.
18 U.S.C.A. § 175b Possession of Biological Weapons by Restricted Persons	October 26, 2001	Fine, up to 10 years imprisonment or both.
18 U.S.C.A. § 229 Development, Possession, or Transportation of Chemical Weapons	October 21, 1998	Fine, up to 10 years imprisonment, or both (death or life imprisonment if death of another person results from the prohibited action).
18 U.S.C.A. § 1387 Demonstrations at Cemeteries Under Control of the National Cemetery Administration and at Arlington National Cemetery	May 29, 2006	Fine, up to 1 year imprisonment, or both.
18 U.S.C.A. § 1388 Disruption of Funerals of Members or Former Members of the Armed Forces	August 6, 2012	Fine, up to 1 year imprisonment, or both.
18 U.S.C.A. § 1831 Economic Espionage	January 14, 2013	Fine of up to $5 M, up to 15 years imprisonment, or both.
18 U.S.C.A. § 831 Prohibited Transactions Involving Nuclear Materials	June 2, 2015	The punishment for an offense under-- (1) paragraphs (1) through (8) of subsection (a) of this section is-- (A) a fine under this title; and (B) imprisonment-- (i) for any term of years or for life (I) if, while committing the offense, the offender knowingly causes the death of any person; or (II) if, while committing an offense under paragraph (1) or (3) of

		subsection (a) of this section, the offender, under circumstances manifesting extreme indifference to the life of an individual, knowingly engages in any conduct and thereby recklessly causes the death of or serious bodily injury to any person; and (ii) for not more than 20 years in any other case; and (2) paragraph (9) of subsection (a) of this section is-- (A) a fine under this title; and (B) imprisonment-- (i) for not more than 20 years if the offense which is the object of the conspiracy is punishable under paragraph (1) (B) (i); and (ii) for not more than 10 years in any other case.
18 U.S.C.A. § 832 Participation in Nuclear and Weapons of Mass Destruction Threats to the United States	December 17, 2004	Imprisonment for any term of years or for life.
18 U.S.C.A. § 836 Transportation of Fireworks into State Prohibiting Sale or Use	July 1, 1954	Fine, up to 1 year imprisonment, or both.
18 U.S.C.A. § 842 Importation, Manufacture, Distribution, and Storage of Explosive Materials	December 13, 2003	(a) Any person who-- (1) violates any of subsections (a) through (i) or (l) through (o) of section 842 shall be fined under this title, imprisoned for not more than 10 years, or both; and (2) violates subsection (p)(2) of section 842, shall be fined under this title, imprisoned not more than 20 years, or both. (b) Any person who violates any other provision of section 842 of this chapter shall be fined under this title or imprisoned not more than one year, or both.
18 U.S.C.A. § 2332a Use of Weapons of Mass Destruction	December 17, 2004	Imprisonment for any term of years or for life and if death results, death or

		imprisonment for any term of years or life.
18 U.S.C.A. § 2332b Acts of Terrorism Transcending National boundaries	June 2, 2015	Whoever violates this section shall be punished-- (A) for a killing, or if death results to any person from any other conduct prohibited by this section, by death, or by imprisonment for any term of years or for life; (B) for kidnapping, by imprisonment for any term of years or for life; (C) for maiming, by imprisonment for not more than 35 years; (D) for assault with a dangerous weapon or assault resulting in serious bodily injury, by imprisonment for not more than 30 years; (E) for destroying or damaging any structure, conveyance, or other real or personal property, by imprisonment for not more than 25 years; (F) for attempting or conspiring to commit an offense, for any term of years up to the maximum punishment that would have applied had the offense been completed; and (G) for threatening to commit an offense under this section, by imprisonment for not more than 10 years.
18 U.S.C.A. § 2332f Bombings of Places of Public Use, Government Facilities, Public Transportation Systems, and Infrastructure Facilities	June 25, 2002	Imprisonment for any term of years or for life and if death results, death or imprisonment for any term of years or life.
18 U.S.C.A. § 2332g Missile Systems Designed to Destroy Aircraft	December 17, 2004	(1) In general.--Any person who violates, or attempts or conspires to violate, subsection (a) shall be fined not more than $2,000,000 and shall be sentenced to a term of imprisonment not less than 25 years or to imprisonment for life. (2) Other circumstances.--Any person who, in the course of a violation of subsection (a), uses, attempts or conspires to use, or possesses and threatens to use, any item or items described in subsection (a), shall be

		fined not more than $2,000,000 and imprisoned for not less than 30 years or imprisoned for life. (3) Special circumstances.--If the death of another results from a person's violation of subsection (a), the person shall be fined not more than $2,000,000 and punished by imprisonment for life.
18 U.S.C.A. § 2332h Use of Radiological Dispersal Devices	December 17, 2004	(1) In general.--Any person who violates, or attempts or conspires to violate, subsection (a) shall be fined not more than $2,000,000 and shall be sentenced to a term of imprisonment not less than 25 years or to imprisonment for life. (2) Other circumstances.--Any person who, in the course of a violation of subsection (a), uses, attempts or conspires to use, or possesses and threatens to use, any item or items described in subsection (a), shall be fined not more than $2,000,000 and imprisoned for not less than 30 years or imprisoned for life. (3) Special circumstances.--If the death of another results from a person's violation of subsection (a), the person shall be fined not more than $2,000,000 and punished by imprisonment for life.
18 U.S.C.A. § 2332i Acts of Nuclear Terrorism	June 2, 2015	Fine of up to $2 M and imprisonment for any term of years or for life.
49 U.S.C.A. § 46306 Registration Violations Involving Aircraft Not Providing Air Transportation	July 5, 1994	Fine and imprisonment up to 3 years as a general criminal penalty; if the offense is related to transporting a controlled substance, a fine and imprisonment up to 5 years or both.
49 U.S.C.A. § 43607 Violation of National Defense Space	July 5, 1994	Fine and imprisonment up to 1 year or both.
49 U.S.C.A. § 43608 Interference With Air Navigation	July 5, 1994	Fine and imprisonment up to 5 years or both.
49 U.S.C.A. § 43612 Transporting Hazardous Material	July 5, 1994	Fine and imprisonment up to 5 years or both.

49 U.S.C.A. § 43613 Refusing to Appear or Produce Records	July 5, 1994	Fine and imprisonment up to 1 year or both.
49 U.S.C.A § 43615 Lighting Violations Involving Transporting Controlled Substances by Aircraft Not Providing Air Transportation	July 5, 1994	Fine and imprisonment up to 5 years or both.
54 U.S.C.A. § 100751 National Park Service Regulations; 18 U.S.C.A. § 1865 Penalties	December 19, 2014	Fine and imprisonment up to six months.

STATE DRONE CHART

State	Statute	Date Enacted	Class of Offense/Civil Remedy
Alaska	AS § 18.65.901 Law Enforcement Operational Requirements for Unmanned Aircraft Systems	October 26, 2014	N/A
Alaska	AS § 18.65.902 Use of an Unmanned Aircraft System by a Law Enforcement Agency	October 26, 2014	N/A
Alaska	AS § 18.65.903 Retention of Images Captured by an Unmanned Aircraft System by Law Enforcement	October 26, 2014	N/A
Alaska	AS § 18.65.900 Law Enforcement May Only Use Unmanned Aircraft Systems in Accordance with State Statutes	October 26, 2014	N/A
Alaska	AS § 29.35.146 Prohibiting Municipalities from Adopting Ordinance Permitting the Release of Images Captured by Law Enforcement Using an Unmanned Aircraft System in a Manner Inconsistent with State Statutes	October 26, 2014	N/A
Arkansas	A.C.A. § 5-60-103 Prohibiting the Use of an Unmanned Aircraft System to Conduct Surveillance Of, Gather Evidence or Collect Information About, or Photographically or Electronically Record	July 22, 2015	Class B Misdemeanor (Class A Misdemeanor for Second of Subsequent Offense). Offenders are civilly liable to the owner of the infrastructure in question for

	Critical Infrastructure Without the Prior Written Consent of its Owner		(1) Any actual damages sustained as a result of the violation, or ten thousand dollars ($10,000), whichever is greater; (2) Three (3) times actual damages, or ten thousand dollars ($10,000), whichever is greater, in a case in which the violation resulted in profit or monetary gain; and (3) The costs of an action brought under this section, together with reasonable attorney's fees as determined by the court.
Arkansas	A.C.A. § 5-16-102 Voyeurism Including the Use of Unmanned Aircraft Systems	July 22, 2015	Class A Misdemeanor (Class D Felony if victim is under 17 years of age and the offender holds a position of trust or authority over the victim).
Arkansas	A.C.A. § 5-16-101 Video Voyeurism Including the Use of Unmanned Aircraft Systems	July 22, 2015	(c)(1) A violation of subsection (a) of this section is a Class D felony. (2)(A) A violation of subsection (b) of this section is a Class B misdemeanor. (B) However, a violation of subsection (b) of this section is a Class A misdemeanor if: (i) The person who created the video recording, film, or photo obtained as described in subsection

			(b) of this section distributed or transmitted it to another person; or (ii) The person who created the video recording, film, or photo obtained as described in subsection (b) of this section posted it in a format accessible by another person via the Internet.
California	§ 21646 Flying or Releasing Balloon, Kite, or Rocket Near Airport	1970	Misdemeanor
Delaware	§ 4504 Utility Companies and Governmental Agencies May Be Issued a Permit for a Manned and/or Unmanned Aerial Type Single Motor vehicle up to 50 Feet Long.	1984	N/A
Florida	§ 934.50 Prohibition of Searches and Seizure Using a Drone: Law enforcement may not use drones to gather evidence or other information and a person, a state agency, or political subdivision may not use a drone equipped with an imaging device to record an image of privately owned real property or its owner, occupant, invitee or licensee with the intent to conduct surveillance without his or her written consent. The statute permits the use of drones:	July 1, 2015	Aggrieved parties may initiate civil actions against law enforcement agencies to obtain all appropriate relief in order to prevent or remedy a violation of the section.

	(a) To counter a high risk of a terrorist attack by a specific individual or organization if the United States Secretary of Homeland Security determines that credible intelligence indicates that there is such a risk. (b) If the law enforcement agency first obtains a search warrant signed by a judge authorizing the use of a drone. (c) If the law enforcement agency possesses reasonable suspicion that, under particular circumstances, swift action is needed to prevent imminent danger to life or serious damage to property, to forestall the imminent escape of a suspect or the destruction of evidence, or to achieve purposes including, but not limited to, facilitating the search for a missing person. (d) By a person or an entity engaged in a business or profession licensed by the state, or by an agent, employee, or contractor thereof, if the drone is used only to perform reasonable tasks within the scope of practice or activities permitted under such person's or entity's license. However, this exception does not apply to a profession in which the		

	licensee's authorized scope of practice includes obtaining information about the identity, habits, conduct, movements, whereabouts, affiliations, associations, transactions, reputation, or character of any society, person, or group of persons. (e) By an employee or a contractor of a property appraiser who uses a drone solely for the purpose of assessing property for ad valorem taxation. (f) To capture images by or for an electric, water, or natural gas utility: 1. For operations and maintenance of utility facilities, including facilities used in the generation, transmission, or distribution of electricity, gas, or water, for the purpose of maintaining utility system reliability and integrity; 2. For inspecting utility facilities, including pipelines, to determine construction, repair, maintenance, or replacement needs before, during, and after construction of such facilities; 3. For assessing vegetation growth for the purpose of maintaining clearances on utility rights-of-way;		

	4. For utility routing, siting, and permitting for the purpose of constructing utility facilities or providing utility service; or 5. For conducting environmental monitoring, as provided by federal, state, or local law, rule, or permit. (g) For aerial mapping, if the person or entity using a drone for this purpose is operating in compliance with Federal Aviation Administration regulations. (h) To deliver cargo, if the person or entity using a drone for this purpose is operating in compliance with Federal Aviation Administration regulations. (i) To capture images necessary for the safe operation or navigation of a drone that is being used for a purpose allowed under federal or Florida law.		
Idaho	I.C. § 21-213 Restriction on Use of Unmanned Aircraft Systems: Absent a warrant, and except for emergency response for safety, search and rescue or controlled substance investigations, no person, entity or state agency shall use an unmanned aircraft system to intentionally conduct surveillance of, gather evidence or collect information about, or photographically or	July 1, 2013	(3) Any person who is the subject of prohibited conduct under subsection (2) of this section shall: (a) Have a civil cause of action against the person, entity or state agency for such prohibited conduct; and (b) Be entitled to recover from any such person, entity or state agency damages in the amount of the greater

	electronically record specifically targeted persons or specifically targeted private property including, but not limited to: (i) An individual or a dwelling owned by an individual and such dwelling's curtilage, without such individual's written consent; (ii) A farm, dairy, ranch or other agricultural industry without the written consent of the owner of such farm, dairy, ranch or other agricultural industry. (b) No person, entity or state agency shall use an unmanned aircraft system to photograph or otherwise record an individual, without such individual's written consent, for the purpose of publishing or otherwise publicly disseminating such photograph or recording. (4) An owner of facilities located on lands owned by another under a valid easement, permit, license or other right of occupancy is not prohibited in this section from using an unmanned aircraft system to aerially inspect such facilities.		of one thousand dollars ($1,000) or actual and general damages, plus reasonable attorney's fees and other litigation costs reasonably incurred.
Illinois	20 ILCS 5065/15 Unmanned Aerial System Task Force was created to study and make	August 18, 2015	N/A

	recommendations for the operation, usage, and regulation of unmanned aerial systems within the state. The task force shall submit a report with recommendations to the Governor and General Assembly by July 1, 2016.		
Indiana	IC 14-22-6-16 Prohibition Against the Use of an Unmanned Aerial Vehicle to Aid in the Taking of an Animal: a person may not knowingly use an unmanned aerial vehicle to search for, scout, locate, or detect a wild animal to which the hunting season applies as an aid to take the wild animal.	March 22, 2016	$20 fine for first violation, $35 fine for each subsequent violation.
Indiana	IC 35-33-5-9 Search Warrant Requirement for the Use of Unmanned Aerial Vehicles Sec. 9. (a) Except as provided in subsection (b), a law enforcement officer must obtain a search warrant in order to use an unmanned aerial vehicle. (b) A law enforcement officer or governmental entity may use an unmanned aerial vehicle without obtaining a search warrant if the law enforcement officer determines that the use of the unmanned aerial vehicle: (1) is required due to: (A) the existence of exigent circumstances necessitating a warrantless search;	March 21, 2016	Evidence obtained in violation of the statute is inadmissible in administrative or judicial proceedings.

	(B) the substantial likelihood of a terrorist attack; (C) the need to conduct a search and rescue or recovery operation; (D) the need to conduct efforts: (i) in response to; or (ii) to mitigate; the results of a natural disaster or any other disaster; or (E) the need to perform a geographical, an environmental, or any other survey for a purpose that is not a criminal justice purpose; (2) is required to obtain aerial photographs or video images of a motor vehicle accident site on a public street or public highway; or (3) will be conducted with the consent of any affected property owner.		
Iowa	I.C.A. § 808.15 Warrant Requirement for Unmanned Aerial Vehicle Use.	July 1, 2014	Information obtained as a result of the use of an unmanned aerial vehicle without a search warrant is inadmissible in criminal and civil proceedings.
Iowa	I.C.A. § 321.492B Prohibition of the Use of Unmanned Aerial Vehicles for Traffic Law Enforcement	July 1, 2014	Information obtained through the use of unmanned aerial vehicles for traffic law enforcement is inadmissible in

			criminal and civil proceedings.
Louisiana	LSA-R.S. 3:44 Unmanned Aerial Systems: A. Unmanned aerial systems may operate in agricultural commercial operations in accordance with this Chapter and the rules and regulations established by the commissioner, except as prohibited by federal law. B. (1) Private landowners engaged in agricultural commercial operations on their private property may use unmanned aerial systems within the geographical confines of their property. (2) Producers, tenants, lessees, university researchers, or other contracted or hired personnel working on private property who are engaged in agricultural commercial operations may use unmanned aerial systems within the geographical confines of the property, only with written permission of the landowner or entity controlling the agricultural commercial use of the property. (3) Data obtained through the use of an unmanned aerial system shall be used solely in the course of conducting a generally accepted agricultural commercial operation, or in conjunction with an	June 23, 2015	N/A

	agricultural research, extension program, or initiative conducted by a Louisiana public postsecondary educational institution. (4) All data obtained through the use of an unmanned aerial system shall remain the property of the legal owner of the property where the data was collected, unless written approval is given by the property owner for other uses. Public universities conducting agricultural research may negotiate with the legal owner of the property for the terms of use or shared ownership of the data.		
Louisiana	LSA-R.S. 14:337 Unlawful Use of an Unmanned Aircraft System: Unlawful use of an unmanned aircraft system is the intentional use of an unmanned aircraft system to conduct surveillance of, gather evidence or collect information about, or photographically or electronically record a targeted facility (petroleum and alumina refineries, chemical and rubber manufacturing facilities, nuclear power electric generation facilities) without the prior written consent of the owner of the	August 1, 2014	Misdemeanor

	targeted facility. The statute only applies to non-governmental operators of such aircraft systems.		
Maine	25 M.R.S.A. § 4501 Regulation of Unmanned Aerial Vehicles; 4. Law enforcement agency operation of unmanned aerial vehicles. A law enforcement agency's operation of an unmanned aerial vehicle must fully comply with all Federal Aviation Administration requirements and guidelines, including the acquisition of a certificate of authorization or waiver from the Federal Aviation Administration. Additionally, a law enforcement agency's use of an unmanned aerial vehicle is governed by the following provisions. A. A law enforcement agency may not use an unmanned aerial vehicle before adopting standards that meet, at a minimum, the standards set forth in subsection 5. B. Except as permitted by a recognized exception to the requirement for a warrant under the Constitution of Maine or the United States Constitution, a law enforcement agency may not use an unmanned aerial vehicle for criminal investigations without a warrant.	October 15, 2015	N/A

	C. Notwithstanding paragraph A, a law enforcement agency may use an unmanned aerial vehicle for the purpose of a search and rescue operation when the law enforcement agency determines that use of an unmanned aerial vehicle is necessary to alleviate an immediate danger to any person or for training exercises related to such uses. D. Notwithstanding paragraph A, a law enforcement agency may use an unmanned aerial vehicle for purposes other than the investigation of crime, including, but not limited to, aerial photography for the assessment of accidents, forest fires and other fire scenes, flood stages and storm damage. E. In no case may a weaponized unmanned aerial vehicle be used or its use facilitated by a state or local law enforcement agency in this State. F. A law enforcement agency may not use an unmanned aerial vehicle to conduct surveillance of private citizens peacefully exercising their constitutional rights of free speech and assembly.		

	G. Notwithstanding paragraph A, a law enforcement agency may use an unmanned aerial vehicle for an emergency use approved by the chief administrative officer of the agency or the Governor 5. Minimum standards for law enforcement. The Board of Trustees of the Maine Criminal Justice Academy, in consultation with the Office of the Attorney General, shall establish minimum standards for written policies and protocols for use of unmanned aerial vehicles by law enforcement agencies. The standards must include at a minimum: A. Training and certification requirements for a person operating an unmanned aerial vehicle; B. Requirements for prior authorization for the use of an unmanned aerial vehicle by the chief administrative officer of the law enforcement agency seeking to use such a vehicle; C. Approval by the Attorney General or chief prosecuting attorney for the appropriate jurisdiction for the deployment of an unmanned aerial vehicle for criminal investigation purposes; D. Restrictions on the use of night vision technology, high-powered zoom lenses,		

	video analytics, facial recognition technology, thermal imaging and other such enhancement technology; E. Procedures to minimize the inadvertent audio or visual recording of private spaces of 3rd parties who are not under investigation; F. Procedures for destroying any unnecessary audio or visual recordings without further duplication or dissemination; G. Recommended minimum altitudes and speeds at which an unmanned aerial vehicle may be flown in order to minimize the invasion of privacy of 3rd parties who are not under investigation; H. Methods to minimize the number of unmanned aerial vehicles deployed at any one time in any one area or at any one event; I. Procedures to avoid hazards to persons and property on land and in the air due to the operation of unmanned aerial vehicles; J. Methods for tracking and recording the flight of each unmanned aerial vehicle; K. Requirements for regular statistical reporting of all uses of unmanned aerial vehicles, including the purposes, the results		

	and the duration of such uses, to the appropriate governmental bodies; and L. Accountability of a law enforcement agency for any mistake in deployment or misuse of an unmanned aerial vehicle, including sanctions as provided in section 2803-C or section 2806-A, as applicable.		
Maryland	§ 14-301 Laws Governing the Testing and Operation of Unmanned Aircraft Systems: Only the state may prohibit, restrict, or regulate the testing or operation of unmanned aircraft systems	July 1, 2015	N/A
Michigan	M.C.L.A.324.40111c: Prohibition on Taking Fish or Game Using Unmanned Aerial Vehicles	July 13, 2015	Misdemeanor
Michigan	M.C.L.A. 324.40112 Prohibition on Using Unmanned Aerial Vehicles to interfere with the Lawful Taking of Fish and Game by Another	July 13, 2015	Misdemeanor
Mississippi	§ 97-29-61: Voyeurism Including the Use of Drones	July 1, 2015	Felony
Montana	MCA 46-5-109 Prohibition on the Use of Information Obtained Using Unmanned Aerial Vehicles Unless Obtained Pursuant to a Search Warrant or Judicially Recognized Exceptions to the Warrant Requirement or Monitoring of Public Lands or International Borders. Information obtained using unmanned aerial vehicles may not be	October 1, 2013	Information obtained in violation of the statute is inadmissible in judicial proceedings.

	used to obtain search warrants unless it is obtained pursuant to a search warrant, a judicially recognized exception to the warrant requirement, or through monitoring of public lands and international borders.		
Montana	MCA 7-32-401: Prohibition on Law Enforcement Receiving Drones that are Armored, Weaponized or Both from a Federal Military Equipment Surplus Program.	October 1, 2015	N/A
Nevada	N.R.S. 493.130 Operation of Aircraft While Under Influence of Intoxicating Liquor or Controlled Substance or in Reckless Manner (Including Unmanned Aerial Vehicles)	October 1, 2015	Gross Misdemeanor
Nevada	N.R.S. 493.100 Dangerous Flying (Applies to Unmanned Aerial Vehicles if the Operator Operates it With Reckless Disregard for the safety of Other Persons and With Willful Indifference to Injuries that Could Reasonably Result from Such Operation.	October 1, 2015	Misdemeanor
Nevada	N.R.S. 493.109 Prohibition on the Operation of Unmanned Aerial Vehicles Within 5 miles of an Airport Without the Airport Operator's Consent or Within 500 Feet Horizontal Distance	October 1, 2015	Misdemeanor

	or 250 Feet Vertical Distance from a Critical Facility Without the Written Consent of the Facility's Owner		
Nevada	N.R.S. 493.106 Prohibition on Weaponizing Unmanned Aerial Vehicles	October 1, 2015	Category C Felony
Nevada	N.R.S. 493.118 Requiring the State to Establish and Maintain a Registry of Unmanned Aerial Vehicles Operated by Public Agencies	October 1, 2015	N/A
Nevada	N.R.S. 493.112 Prohibiting Warrantless Operation of Unmanned Aerial Vehicles by Law Enforcement for the Purpose of Gathering Evidence from Properties at Which People have a Reasonable Expectation of Privacy Unless Exigent Circumstances to Search Warrant Requirements Exist	October 1, 2015	Evidence gathered in violation of the statute is inadmissible in any adjudicatory proceeding.
Nevada	N.R.S. 493.115 Prohibiting the Operation of Unmanned Aerial Vehicles by Public Agencies Unless (1) Before the operation of the unmanned aerial vehicle, the public agency registers the unmanned aerial vehicle with the Department pursuant to subsection 2 of NRS 493.118. (2) The public agency operates the unmanned aerial vehicle in accordance with the regulations adopted by the Department pursuant to subsection 4 of NRS 493.118.	October 1, 2015	Information obtained in violation of the statute is inadmissible in an adjudicatory proceeding.

	(b) Must not operate an unmanned aerial vehicle for the purposes of assisting a law enforcement agency with law enforcement or conducting a criminal prosecution.		
Nevada	N.R.S. 493.103 Trespass Using Unmanned Aerial Vehicles: 1. Except as otherwise provided in subsection 2, a person who owns or lawfully occupies real property in this State may bring an action for trespass against the owner or operator of an unmanned aerial vehicle that is flown at a height of less than 250 feet over the property if: (a) The owner or operator of the unmanned aerial vehicle has flown the unmanned aerial vehicle over the property at a height of less than 250 feet on at least one previous occasion; and (b) The person who owns or occupies the real property notified the owner or operator of the unmanned aerial vehicle that the person did not authorize the flight of the unmanned aerial vehicle over the property at a height of less than 250 feet. For the purposes of this paragraph, a person may place the owner or	October 1, 2015	A plaintiff who prevails in an action for trespass brought pursuant to subsection 1 is entitled to recover treble damages for any injury to the person or the real property as the result of the trespass. In addition to the recovery of damages pursuant to this subsection, a plaintiff may be awarded reasonable attorney's fees and costs and injunctive relief.

	operator of an unmanned aerial vehicle on notice in the manner prescribed in subsection 2 of NRS 207.200. 2. A person may not bring an action pursuant to subsection 1 if: (a) The unmanned aerial vehicle is lawfully in the flight path for landing at an airport, airfield or runway. (b) The unmanned aerial vehicle is in the process of taking off or landing. (c) The unmanned aerial vehicle was under the lawful operation of: (1) A law enforcement agency in accordance with NRS 493.112. (2) A public agency in accordance with NRS 493.112 (d) The unmanned aerial vehicle was under the lawful operation of a business registered in this State or a land surveyor if: (1) The operator is licensed or otherwise approved to operate the unmanned aerial vehicle by the Federal Aviation Administration; (2) The unmanned aerial vehicle is being operated within the scope of the lawful activities of the business or surveyor; and (3) The operation of the unmanned aerial vehicle does not unreasonably interfere with the existing use of the real property.		

New Hampshire	N.H. Rev. Stat. § 207:57 Prohibition on the Use of Unmanned Aerial Vehicles to Conduct Video Surveillance of Private Citizens Lawfully Hunting, Fishing, or Trapping Without Obtaining Their Written Consent	January 1, 2016	Misdemeanor
North Carolina	N.C.G.S.A. § 113-295 Prohibition on the Use of Unmanned Aircraft Systems to Intentionally Interfere With the Lawful Taking of Wildlife Resources.	December 1, 2014	Class 1 Misdemeanor
North Carolina	N.C.G.S.A. § 14-280.3 Prohibition on Intentional Interference With Manned Aircraft Using Unmanned Aerial Vehicles.	December 1, 2014	Class H Felony
North Carolina	N.C.G.S.A. § 15A-300.2 Prohibition on the Launch or Recovery of Unmanned Aerial Vehicles from State or Private Property Without Consent	October 1, 2014	Misdemeanor
North Carolina	N.C.G.S.A. § 14-7.45 All Crimes Committed Using an Unmanned Aircraft System While in Flight Over North Carolina are Governed by North Carolina Law.	December 1, 2014	N/A
North Carolina	N.C.G.S.A. § 63-95 No Agent of the state May Operate an Unmanned Aircraft System Without Completion of a Test Administered by the Division of Aviation of the State Department of Transportation.	August 25, 2015	N/A

North Carolina	N.C.G.S.A. § 14-401.24 Prohibition on the Possession or Use of Weaponized Unmanned Aircraft Systems and the use of Unmanned Aircraft Systems to Hunt or Fish	December 1, 2014	Class E Felony (possession or use of weaponized unmanned aircraft system) Class 1 Misdemeanor (hunting using an unmanned aircraft system)
North Carolina	N.C.G.S.A. § 63-96 Requiring Permits for the Operation of Unmanned Aerial Vehicles for Commercial Purposes: in order to receive a permit an individual must be at least 17 years of age, possess a valid drivers' license, and pass a prescribed test.	August 25, 2015	Class 1 Misdemeanor
North Carolina	N.C.G.S.A. § 15A-300.1 Prohibiting Private Individuals and Entities and State Agencies from Using Unmanned Aircraft Systems to: conduct surveillance of a person, occupied dwelling, or private real property without the owner or lessee's consent or photographing an individual without their consent for the purpose of publishing or publically disseminating the photograph with the exception of newsgathering, newsworthy events, or events or places to which the general public is invited.	October 1, 2014	Evidence obtained in violation of the statute is inadmissible in any proceedings. People who are the subject of surveillance or are photographed in violation of the statute have a civil cause of action against the actor and may recover $5,000 per photograph or video in addition to reasonable costs and attorneys' fees in the absence of actual damages.
Oregon	O.R.S. § 163.700 Invasion of Personal Privacy in the Second Degree Including	March 29, 2016	Class A Misdemeanor

	the Use of Unmanned Aerial Vehicles		
Oregon	Ch. 72, § 5 Prohibition on Recklessly Causing an Unmanned Aircraft System to Direct a Laser at an Airborne Aircraft, Crash into an Airborne Aircraft, or Prevent the Takeoff or Landing of an Aircraft	March 29, 2016	Class A Misdemeanor
Oregon	O.R.S. § 498.128 Prohibiting the Use of Drones for Hunting, Trapping, or Fishing, or Interfering With Lawful Hunting, Trapping, or Fishing.	January 1, 2016	Violation of State Fish and Wildlife Commission Regulations
Oregon	Ch. 72, § 13 Prohibiting the Deliberate Operation of an Unmanned Aircraft System less than 400 feet Above a Critical Infrastructure Facility Without its Owner's Consent.	March 29, 2016	Class A Misdemeanor
Oregon	O.R.S. § 837.995 Prohibiting Operators of Unmanned Aerial Vehicles From Intentionally Causing Such Devices to Fire Bullets or Projectiles at Airborne Aircraft, Direct Lasers at Airborne Aircraft, or Crash into Airborne Aircraft	July 29, 2013	Class A Felony
Oregon	O.R.S. § 837.375 Prohibiting Intentional Intereference With Unmanned Aircraft Systems licensed by the FAA or operated by the Federal Government	July 29, 2013	Civil liability to the device's owner (at least $5,000 in addition to reasonably attorney fees.

Oregon	O.R.S. § 837.365 Prohibiting the Operation of Weaponized Unmanned Aircraft Systems	March 29, 2016	Class A Misdemeanor
Oregon	O.R.S. § 837.385 Prohibiting Local Government Regulation of Unmanned Aerial Vehicles Except as Expressly Authorized by State Statute	July 29, 2013	N/A
Oregon	O.R.S. § 837.310 Prohibiting Law Enforcement Use of Unmanned Aircraft Systems in Violation of State Statutes	January 1, 2016	Evidence obtained in violation of the statute is inadmissible in judicial or administrative proceedings.
Oregon	O.R.S. § 837.330 Law Enforcement Agencies May Operate Unmanned Aircraft Systems for the Purpose of Acquiring Information About an Individual or the Individual's Property With the Individual's Written Consent	July 29, 2013	N/A
Oregon	O.R.S. § 837.340 Law Enforcement Agencies May Use Unmanned Aircraft Systems to Reconstruct Crime Scenes	July 29, 2013	N/A
Oregon	O.R.S. § 837.360 Prohibiting Public Bodies from Operating Unmanned Aircraft Systems Without Registering them with the State Department of Aviation	January 2, 2016	$10,000 fine
Oregon	O.R.S. § 837.380 Permitting Property Owners and Lawful Occupants to Bring Civil Action Against Anyone Who Files an Unmanned Aerial System Over the	July 29, 2013	Civil remedies include damages, injunctive relief, and attorney fees (if damages are $10,000 or less).

	Property if the Operator Previously Flew it Over the Property in Question and the Owner or Occupier Notified the Operator He Did not Want it Flown over the Property		
Oregon	O.R.S. § 837.345 Images and Information Acquired Through the Warrantless Use of Unmanned Aircraft Systems by Law Enforcement are Inadmissible in Adjudicatory Proceedings and May not be Used to Establish Reasonable Suspicion or Probable Cause to Believe an Offense has been Committed; Authorizing Law Enforcement Agencies to Operate Unmanned Aircraft Systems for Training.	July 29, 2013	Information obtained in violation of the statute is inadmissible.
Oregon	O.R.S. § 837.320 Authorizes Law Enforcement to Operate an Unmanned Aircraft System to Obtain Information Pursuant to a Warrant, Probable Cause, or Exigent Circumstances.	July 29, 2013	Information obtained in violation of the statute is inadmissible.
Oregon	O.R.S. § 837.335 Authorizes Law Enforcement Use of Unmanned Aircraft Systems for Search and Rescue, Emergency Assistance, and States of Emergency	July 29, 2013	N/A
Tennessee	T. C. A. § 39-14-405 Defines Unmanned	July 1, 2014	Class C Misdemeanor

	Aircraft Systems' Presence on Private Property Without the Owner's Consent as Criminal Trespass.		
Tennessee	T. C. A. § 39-13-904 Prohibits the Use of Unmanned Aircraft Systems to Photograph or Videotape People Without Their Consent	July 1, 2014	Class C Misdemeanor (Class B Misdemeanor for disclosing, displaying, distributing, or otherwise using an image or video obtained in violation of the statute)
Tennessee	T. C. A. § 39-13-905 Images Captured by Unmanned Aircraft of Privately Owned Real Property, Open-Air Venues with More than 100 Individuals Present Without Owner or Operator's Consent, or Fireworks Display or Discharge Sites May Not be Used as Evidence in Adjudicative Proceedings	July 1, 2014	Evidence obtained in violation of the statute is inadmissible in adjudicative proceedings.
Tennessee	T. C. A. § 39-13-902 Authorizes the Capture of Images Using Unmanned Aircraft under the Following Circumstances: (1) For purposes of professional or scholarly research and development by a person acting on behalf of an institution of higher education, as defined by § 49-7-802, including a person who: (A) Is a professor, employee, or student of the institution; or (B) Is under contract with or otherwise acting under the direction or on behalf of the institution;	July 1, 2014	N/A

	(2) In airspace designated as a test site or range authorized by the federal aviation administration for the purpose of integrating unmanned aircraft systems into the national airspace; (3) As part of an authorized operation, exercise, or mission of any branch of the United States military, consistent with the Constitution of the United States; (4) If the image is captured for the purposes of mapping; provided, the image of any person or thing on private property captured in the course of mapping shall be subject to subdivision (a)(6) as an image captured incidental to the lawful capturing of an image; (5) If the image is captured by or for an electric or natural gas utility: (A) For operations and maintenance of utility facilities for the purpose of maintaining utility system reliability and integrity (B) For inspecting utility facilities to determine repair, maintenance, or replacement needs during and after construction of such facilities; (C) For assessing vegetation growth for the purpose of maintaining		

	clearances on utility easements; or (D) For utility facility routing and siting for the purpose of providing utility service (6) With the consent of the individual who owns or lawfully occupies the real property captured in the image; (7) For law enforcement purposes, as permitted by § 39-13-609; (8) If the image is captured by state or local law enforcement authorities, or a person who is under contract with or otherwise acting under the direction or on behalf of state authorities, for the purpose of: (A) Surveying the scene of a catastrophe or other damage to determine whether a state of emergency should be declared; (B) Preserving public safety, protecting property, or surveying damage or contamination during a lawfully declared state of emergency; or (C) Conducting routine air quality sampling and monitoring, as provided by state or local law; (9) At the scene of a spill, or a suspected spill, of hazardous materials (10) For the purpose of fire suppression; (11) For the purpose of rescuing a person whose		

	life or well-being is in imminent danger; (12) If the image is captured by a Tennessee licensed real estate broker in connection with the marketing, sale, or financing of real property, provided that no individual is identifiable in the image; (13) Of public real property or a person on that property; (14) If the image is captured by the owner, operator or agent, or a person under contract with the owner, operator or agent, of an oil, gas, water, or other pipeline for the purpose of inspecting, maintaining, or repairing pipelines or other related facilities, and is captured without the intent to conduct surveillance on an individual or real property located in this state; (15) In connection with oil and gas pipeline and well safety and protection; (16) In connection with port authority surveillance and security; (17) As authorized or permitted by the federal aviation administration for use in a motion picture, television or similar production where the filming is authorized by the property owner and a		

	state or local film permit agency, if required; or (18) As a part of a commercial service that has received authorization from the federal aviation administration to use unmanned aircraft or an unmanned aircraft operating under regulations promulgated by the federal aviation administration for commercial use of unmanned aircraft. (b) An image captured by a state or local government agency, or by a person who is under contract with or otherwise acting under the direction or on behalf of such agency, shall be handled in accordance with § 39-13-609 and shall not be used for any purpose other than the lawful purpose for which the image was captured as permitted by this section.		
Tennessee	T. C. A. § 39-13-903 Prohibiting the Use of Unmanned Aircraft to Capture an Image of an Individual or Privately Owned Real Property, an Individual or Event at an Open-Air Venue with more than 100 Individuals Gathered, or a Designated Fireworks Display, Discharge, or Fallout Area	July 1, 2015	Class C Misdemeanor
Texas	V.T.C.A., Government Code § 423.006 Prohibiting the Use of Unmanned Aircraft to	September 1, 2013	$5,000 in damages for all images captured in a single incident; $10,000 in damages for disclosure, display,

	Photograph Privately Owned Real Property		distribution, or other use of images captured in a single episode; actual damages if the images are disclosed, displayed, or distributed with malice.
Texas	V.T.C.A., Government Code § 411.062 Authorizes the State Law Enforcement and Security Authority to Either Prohibit the Use of Unmanned Aircraft in the Capitol Complex or Authorize Limited Use of Unmanned Aircraft in the Capitol Complex.	September 1, 2015	N/A
Texas	V.T.C.A., Government Code § 423.005 Prohibits the Introduction of Images Captured by Unmanned Aerial Vehicles in Violation of Statute in Adjudicative Proceedings	September 1, 2013	Evidence obtained in violation of the statute is inadmissible in adjudicative proceedings.
Texas	V.T.C.A., Government Code § 423.002 Authorizes the Capture of Images Using Unmanned Aerial Vehicles under the Following Circumstances: (1) for the purpose of professional or scholarly research and development or for another academic purpose by a person acting on behalf of an institution of higher education or a private or independent institution of higher education, as those terms are defined by Section	September 1, 2015	N/A

	61.003, Education Code, including a person who: (A) is a professor, employee, or student of the institution; or (B) is under contract with or otherwise acting under the direction or on behalf of the institution; (2) in airspace designated as a test site or range authorized by the Federal Aviation Administration for the purpose of integrating unmanned aircraft systems into the national airspace (3) as part of an operation, exercise, or mission of any branch of the United States military; (4) if the image is captured by a satellite for the purposes of mapping; (5) if the image is captured by or for an electric or natural gas utility: (A) for operations and maintenance of utility facilities for the purpose of maintaining utility system reliability and integrity; (B) for inspecting utility facilities to determine repair, maintenance, or replacement needs during and after construction of such facilities; (C) for assessing vegetation growth for the purpose of maintaining clearances on utility easements; and (D) for utility facility routing and siting for the		

	purpose of providing utility service; (6) with the consent of the individual who owns or lawfully occupies the real property captured in the image; (7) pursuant to a valid search or arrest warrant; (8) if the image is captured by a law enforcement authority or a person who is under contract with or otherwise acting under the direction or on behalf of a law enforcement authority: (A) in immediate pursuit of a person law enforcement officers have reasonable suspicion or probable cause to suspect has committed an offense, not including misdemeanors or offenses punishable by a fine only; (B) for the purpose of documenting a crime scene where an offense, not including misdemeanors or offenses punishable by a fine only, has been committed; (C) for the purpose of investigating the scene of: (i) a human fatality; (ii) a motor vehicle accident causing death or serious bodily injury to a person; or (iii) any motor vehicle accident on a state highway or federal interstate or highway;		

	(D) in connection with the search for a missing person; (E) for the purpose of conducting a high-risk tactical operation that poses a threat to human life; or (F) of private property that is generally open to the public where the property owner consents to law enforcement public safety responsibilities; (9) if the image is captured by state or local law enforcement authorities, or a person who is under contract with or otherwise acting under the direction or on behalf of state authorities, for the purpose of: (A) surveying the scene of a catastrophe or other damage to determine whether a state of emergency should be declared (B) preserving public safety, protecting property, or surveying damage or contamination during a lawfully declared state of emergency; or (C) conducting routine air quality sampling and monitoring, as provided by state or local law; (10) at the scene of a spill, or a suspected spill, of hazardous materials (11) for the purpose of fire suppression; (12) for the purpose of rescuing a person whose		

	life or well-being is in imminent danger; (13) if the image is captured by a Texas licensed real estate broker in connection with the marketing, sale, or financing of real property, provided that no individual is identifiable in the image; (14) of real property or a person on real property that is within 25 miles of the United States border; (15) from a height no more than eight feet above ground level in a public place, if the image was captured without using any electronic, mechanical, or other means to amplify the image beyond normal human perception; (16) of public real property or a person on that property; (17) if the image is captured by the owner or operator of an oil, gas, water, or other pipeline for the purpose of inspecting, maintaining, or repairing pipelines or other related facilities, and is captured without the intent to conduct surveillance on an individual or real property located in this state; (18) in connection with oil pipeline safety and rig protection;		

	(19) in connection with port authority surveillance and security; (20) if the image is captured by a registered professional land surveyor in connection with the practice of professional surveying, as those terms are defined by Section 1071.002, Occupations Code, provided that no individual is identifiable in the image; or (21) if the image is captured by a professional engineer licensed under Subchapter G, Chapter 1001, Occupations Code1, in connection with the practice of engineering, as defined by Section 1001.003, Occupations Code, provided that no individual is identifiable in the image.		
Texas	V.T.C.A., Government Code § 423.007 The State Department of Public Safety Shall Adopt Rules and Guidelines for Use of Unmanned Aircrafts by Law Enforcement.	September 1, 2013	N/A
Texas	V.T.C.A., Government Code § 423.008 Requires Each State Law Enforcement Agency and each County or Municipal Law Enforcement Agency Located in a County or Municipality Respectively with a Population Greater than 150,000 that Used an Unmanned Aircraft in the Preceding 24 Months Shall Issue a Written Biannual	September 1, 2013	N/A

	Report that Shall be Available for Public Viewing Including (1) the number of times an unmanned aircraft was used, organized by date, time, location, and the types of incidents and types of justification for the use; (2) the number of criminal investigations aided by the use of an unmanned aircraft and a description of how the unmanned aircraft aided each investigation; (3) the number of times an unmanned aircraft was used for a law enforcement operation other than a criminal investigation, the dates and locations of those operations, and a description of how the unmanned aircraft aided each operation; (4) the type of information collected on an individual, residence, property, or area that was not the subject of a law enforcement operation and the frequency of the collection of this information; and (5) the total cost of acquiring, maintaining, repairing, and operating or otherwise using each unmanned aircraft for the preceding 24 months.		

Texas	V.T.C.A., Government Code § 423.0045 Prohibiting the Intentional Operation of an Unmanned Aircraft Less than 400 Feet Above a Critical Infrastructure Facility, Allowing an Unmanned Aircraft to Make Contact with a Critical Infrastructure Facility, or Allowing an Unmanned Aircraft to Come Within a Distance of a Critical Infrastructure Facility that is Close Enough to Interfere with the Operations of or Cause a Disturbance to the Facility.	September 1, 2015	Class B Misdemeanor (Class A Misdemeanor for repeat offenders)
Utah	2016 Utah Laws Ch. 101 (H.B. 126) Prohibiting the Operation of Unmanned Aircraft Systems within an Area that is Under a Temporary Flight Restriction Issued by the FAA as a result of a Wildland Fire, or an area Designated as a Wildland Fire Scene by a Federal, State, or Local Entity.	March 21, 2016	Class B Misdeamanor (Class A Misdemeanor if the unmanned aircraft system causes an aircraft being used to contain or control a wildland fire to drop a payload or water or fire retardant in the wrong location or land without dropping it). (3rd Degree Felony if the unmanned aircraft system comes into direct physical contact with a manned aircraft). (2nd Degree Felony if the operation of the unmanned aircraft is the proximate cause of a manned aircraft colliding with the ground, a structure, or another manned aircraft).
Utah	U.C.A. 1953 § 63G-18-104 Prohibits Law	May 13, 2014	N/A

	Enforcement Agencies from Using, Copying, or Disclosing Data Collected by an Unmanned Aircraft System on a Person, Structure, or Area that is not a Target and Requires Agencies to Delete Such Information Unless: (a) deleting the data would also require the deletion of data that: (i) relates to the target of the operation; and (ii) is requisite for the success of the operation; (b) the law enforcement agency receives the data: (i) through a court order that: (A) requires a person to release the data to the law enforcement agency; or (B) prohibits the destruction of the data; or (ii) from a person who is a nongovernment actor; (c)(i) the data was collected inadvertently; and (ii) the data appears to pertain to the commission of a crime; (d)(i) the law enforcement agency reasonably determines that the data pertains to an emergency situation; and (ii) using or disclosing the data would assist in remedying the emergency; or		

	(e) the data was collected through the operation of an unmanned aircraft system over public lands outside of municipal boundaries.		
Utah	U.C.A. 1953 § 63G-18-103 Prohibits Law Enforcement Agencies from Obtaining, Receiving, or Using Data Acquired through an Unmanned Aircraft Data System Unless it is Obtained (a) pursuant to a search warrant; (b) in accordance with judicially recognized exceptions to warrant requirements; (c) subject to Subsection (2), from a person who is a nongovernment actor; (d) at a testing site; or (e) to locate a lost or missing person in an area in which a person has no reasonable expectation of privacy. Prohibits Nongovernment Actors from Disclosing Data Acquired Through an Unmanned Aircraft System to a Law Enforcement Agency Unless (a) the data appears to pertain to the commission of a crime; or (b) the nongovernment actor believes, in good faith, that: (i) the data pertains to an imminent or ongoing emergency involving danger of death or serious	May 13, 2014	Information obtained in violation of the statute is inadmissible in an adjudicative proceeding.

	bodily injury to an individual; and (ii) disclosing the data would assist in remedying the emergency. (3) A law enforcement agency that obtains, receives, or uses data acquired under Subsection (1)(d) or (e) shall destroy the data as soon as reasonably possible after the law enforcement agency obtains, receives, or uses the data. (4) A law enforcement agency that operates an unmanned aircraft system under Subsection (1)(d) may not operate the unmanned aircraft system outside of the testing site.		
Utah	U.C.A. 1953 § 63G-18-105 Requires a Law Enforcement Agency that Operated an Unmanned Aircraft System in the Previous Calendar Year to submit a Public Report to the state Department of Public Safety (a) the number of times the law enforcement agency operated an unmanned aircraft system in the previous calendar year; (b) the number of criminal investigations aided by the use of an unmanned aircraft system operated by the law enforcement agency in the previous calendar year;	May 13, 2014	N/A

	(c) a description of how the unmanned aircraft system was helpful to each investigation described in Subsection (1)(b) (d) the frequency with which data was collected, and the type of data collected, by an unmanned aircraft system operated by the law enforcement agency on any person, structure, or area other than a target in the previous calendar year; (e) the number of times a law enforcement agency received, from a person who is not a law enforcement agency, data collected by an unmanned aircraft system; and (f) the total cost of the unmanned aircraft system program operated by the law enforcement agency in the previous calendar year, including the source of any funds used to operate the program.		
Virginia	VA Code Ann. § 19.2-60.1 Requires Search Warrants for the Use of Unmanned Aircraft Systems by Public Bodies	July 1, 2015	Evidence obtained in violation of the statute is inadmissible.
West Virginia	W. Va. Code, § 20-2-5 Prohibits the Use of Unmanned Aircrafts to Hunt, Take, or Kill Wild Animals or Drive or Herd Wild Animals for the Purposes of Hunting, Trapping, or Killing.	June 12, 2015	Misdemeanor
Wisconsin	W.S.A. 942.10 Prohibiting the Use of a Drone With the Intent to Photograph,	April 10, 2014	Class A Misdemeanor

	Record, or Otherwise Observe an Individual in a Place or Location where the Individual has a Reasonable Expectation of Privacy.		
Wisconsin	W.S.A. 941.292 Prohibiting the Possession or Operation of a Weaponized Drone	April 10, 2014	Class H Felony

Note from the Editor . . .

We are pleased to offer the United States Attorneys' Community the first of two issues on the very relevant and timely topic of Forensic Science and Forensic Evidence. Please watch for the second issue in February.

We would like to thank Gretchen C. F. Shappert, Assistant Director, Indian, Violent and Cyber-Crime Staff, Executive Office for United States Attorneys, for her continuing support of the Bulletin, including her leadership on these two issues.

These two issues would not have been possible without the incalculable contributions of Dr. Victor Weedn, who served in 2016 as the Senior Forensic Advisor to then Deputy Attorney General Sally Q. Yates. Dr. Weedn is the former President of the American Academy of Forensic Science and is both a professor and Chair of the George Washington University Department of Forensic Sciences. He founded the Armed Forces DNA Identification Laboratory and holds both a law degree and medical degree.

Dr. Weedn was instrumental in identifying authors for the USA Bulletin Forensic Science issues. He offered inspiration and advice to the writers during the preparation of these issues. Dr. Weedn also worked tirelessly to advise then Deputy Attorney General Yates on a wide variety of forensic science issues and to ensure that the Department of Justice maintains the highest standards of forensic science.

We offer our sincere appreciation and thanks to both Ms. Shappert and Dr. Weedn.

Thank you,

K. Tate Chambers