From: Freeman, Lindsey \(OLP\)
Subject: RE: Contraband cellphones - Court orders (DRAFT)
To: Stawasz, Michael; Sonya Thompson
Cc: Thompson, Sonya \(BOP\); [redacted] \(BOP\); Crytzer, Katherine \(OLP\)
Sent: April 4, 2019 8:54 AM (UTC-04:00)
Attached: Department Policy Memo.pdf

Thanks, Mick. I believe I attached the right policy – let me know if not.

From: Stawasz, Michael <[redacted]>
Sent: Thursday, April 4, 2019 8:37 AM
To: Sonya Thompson <[redacted]>
Cc: Freeman, Lindsey (OLP) <[redacted]>; Thompson, Sonya (BOP) <[redacted]>; [redacted] (BOP) <[redacted]>; Crytzer, Katherine (OLP) <[redacted]>
Subject: Re: Contraband cellphones - Court orders (DRAFT)

CCIPS is the Computer Crime and Intellectual Property Section, my section in the Criminal Division of USDOJ.

The CSS policy was the result of an OLP-led process during the last administration. It sets forth requirements for use of CSS and tasked CCIPS with keeping an agreed template for applications. I will forward a copy when my VPN finally lets me in.

On Apr 4, 2019, at 8:19 AM, Sonya Thompson <[redacted]> wrote:

> Clue me in: who is "CCIPS" and what is the DOJ policy referenced on pages 2-3 re: cell-site simulators?
>
> Is the latter up-to-date in relation to the threats posed by contraband introduction and interdiction (particularly re: phones and drones)? Do we need to add exception use cases?
>
> Sent from my Verizon, Samsung Galaxy smartphone
>
> -------- Original message --------
> From: "Freeman, Lindsey (OLP)" <[redacted]>
> Date: 4/3/19 4:30 PM (GMT-05:00)
> To: "Sonya (BOP) Thompson" <[redacted]>, "[redacted] (BOP)[redacted]" <[redacted]>
> Cc: Michael Stawasz <[redacted]>, Katherine Crytzer <[redacted]>
> Subject: Contraband cellphones - Court orders (DRAFT)
>
> >>> "Freeman, Lindsey (OLP)" 04/03/2019 16:30 >>>
>
> **DRAFT**
>
> [redacted]and Sonya,
>
> Please see CCIPS great work with our comments for tomorrow's meeting at 4:30 pm. Thanks!
>
> Best,
> Lindsey
>
> **Lindsey Freeman**

Acting Chief of Staff
Office of Legal Policy
U.S. Department of Justice
950 Pennsylvania Ave., NW
Washington, DC 20530
Office: (b) (6)
Cell: (b) (6)
(b) (6)

U.S. Department of Justice

Office of the Deputy Attorney General

The Deputy Attorney General

Washington, D.C. 20530

September 3, 2015

MEMORANDUM FOR HEADS OF LAW ENFORCEMENT COMPONENTS

ALL UNITED STATES ATTORNEYS

FROM: Sally Quillian Yates
Deputy Attorney General

SUBJECT: Department Policy Regarding the Use of Cell-Site Simulator Technology

The attached document establishes policy for the Department of Justice regarding the use of cell-site simulator technology. This technology supports critical public safety objectives, such as apprehending fugitives, locating kidnapping victims, and assisting in drug investigations. As with other technological tools, cell-site simulators must be used effectively and in accordance with the law. The attached document establishes consistent policy for the legal process that must be obtained for use of this technology, the information that must be provided to courts in connection with seeking court authority, handling and deletion of data collected by cell-site simulators, and various management and training requirements. The new policy will enhance transparency and accountability, improve our training and supervision, establish a higher and more consistent legal standard, and increase privacy protections in relation to law enforcement's use of this technology.

I ask that you ensure that this policy is shared with all relevant personnel and that appropriate steps are taken to provide the necessary training and ensure compliance with the policy. Any questions regarding this policy should be directed to Samir Jain, Office of the Deputy Attorney General, at (b) (6) [redacted]

Attachment

Department of Justice Policy Guidance: Use of Cell-Site Simulator Technology

Cell-site simulator technology provides valuable assistance in support of important public safety objectives. Whether deployed as part of a fugitive apprehension effort, a complex narcotics investigation, or to locate or rescue a kidnapped child, cell-site simulators fulfill critical operational needs.

As with any law enforcement capability, the Department must use cell-site simulators in a manner that is consistent with the requirements and protections of the Constitution, including the Fourth Amendment, and applicable statutory authorities, including the Pen Register Statute. Moreover, any information resulting from the use of cell-site simulators must be handled in a way that is consistent with the array of applicable statutes, regulations, and policies that guide law enforcement in how it may and may not collect, retain, and disclose data.

As technology evolves, the Department must continue to assess its tools to ensure that practice and applicable policies reflect the Department's law enforcement and national security missions, as well as the Department's commitments to accord appropriate respect for individuals' privacy and civil liberties. This policy provides additional guidance and establishes common principles for the use of cell-site simulators across the Department.[1] The Department's individual law enforcement components may issue additional specific guidance consistent with this policy.

BACKGROUND

Cell-site simulators, on occasion, have been the subject of misperception and confusion. To avoid any confusion here, this section provides information about the use of the equipment and defines the capabilities that are the subject of this policy.

Basic Uses

Law enforcement agents can use cell-site simulators to help locate cellular devices whose unique identifiers are already known to law enforcement, or to determine the unique identifiers of an unknown device by collecting limited signaling information from devices in the simulator user's vicinity. This technology is one tool among many traditional law enforcement techniques, and is deployed only in the fraction of cases in which the capability is best suited to achieve specific public safety objectives.

[1] This policy applies to the use of cell-site simulator technology inside the United States in furtherance of criminal investigations. When acting pursuant to the Foreign Intelligence Surveillance Act, Department of Justice components will make a probable-cause based showing and appropriate disclosures to the court in a manner that is consistent with the guidance set forth in this policy.

How They Function

Cell-site simulators, as governed by this policy, function by transmitting as a cell tower. In response to the signals emitted by the simulator, cellular devices in the proximity of the device identify the simulator as the most attractive cell tower in the area and thus transmit signals to the simulator that identify the device in the same way that they would with a networked tower.

A cell-site simulator receives and uses an industry standard unique identifying number assigned by a device manufacturer or cellular network provider. When used to locate a known cellular device, a cell-site simulator initially receives the unique identifying number from multiple devices in the vicinity of the simulator. Once the cell-site simulator identifies the specific cellular device for which it is looking, it will obtain the signaling information relating only to that particular phone. When used to identify an unknown device, the cell-site simulator obtains signaling information from non-target devices in the target's vicinity for the limited purpose of distinguishing the target device.

What They Do and Do Not Obtain

By transmitting as a cell tower, cell-site simulators acquire the identifying information from cellular devices. This identifying information is limited, however. Cell-site simulators provide only the relative signal strength and general direction of a subject cellular telephone; they do not function as a GPS locator, as they do not obtain or download any location information from the device or its applications. Moreover, cell-site simulators used by the Department must be configured as pen registers, and may not be used to collect the contents of any communication, in accordance with 18 U.S.C. § 3127(3). This includes any data contained on the phone itself: the simulator does not remotely capture emails, texts, contact lists, images or any other data from the phone. In addition, Department cell-site simulators do not provide subscriber account information (for example, an account holder's name, address, or telephone number).

MANAGEMENT CONTROLS AND ACCOUNTABILITY[2]

Cell-site simulators require training and practice to operate correctly. To that end, the following management controls and approval processes will help ensure that only knowledgeable and accountable personnel will use the technology.

1. Department personnel must be trained and supervised appropriately. Cell-site simulators may be operated only by trained personnel who have been authorized by their agency to use the technology and whose training has been administered by a qualified agency component or expert.

[2] This policy guidance is intended only to improve the internal management of the Department of Justice. It is not intended to and does not create any right, benefit, trust, or responsibility, whether substantive or procedural, enforceable at law or equity by a party against the United States, its departments, agencies, instrumentalities, entities, officers, employees, or agents, or any person, nor does it create any right of review in an administrative, judicial, or any other proceeding.

2. Within 30 days, agencies shall designate an executive-level point of contact at each division or district office responsible for the implementation of this policy, and for promoting compliance with its provisions, within his or her jurisdiction.

3. Prior to deployment of the technology, use of a cell-site simulator by the agency must be approved by an appropriate individual who has attained the grade of a first-level supervisor. Any emergency use of a cell-site simulator must be approved by an appropriate second-level supervisor. Any use of a cell-site simulator on an aircraft must be approved either by the executive-level point of contact for the jurisdiction, as described in paragraph 2 of this section, or by a branch or unit chief at the agency's headquarters.

Each agency shall identify training protocols. These protocols must include training on privacy and civil liberties developed in consultation with the Department's Chief Privacy and Civil Liberties Officer.

LEGAL PROCESS AND COURT ORDERS

The use of cell-site simulators is permitted only as authorized by law and policy. While the Department has, in the past, appropriately obtained authorization to use a cell-site simulator by seeking an order pursuant to the Pen Register Statute, as a matter of policy, law enforcement agencies must now obtain a search warrant supported by probable cause and issued pursuant to Rule 41 of the Federal Rules of Criminal Procedure (or the applicable state equivalent), except as provided below.

As a practical matter, because prosecutors will need to seek authority pursuant to Rule 41 *and* the Pen Register Statute, prosecutors should, depending on the rules in their jurisdiction, either (1) obtain a warrant that contains all information required to be included in a pen register order pursuant to 18 U.S.C. § 3123 (or the state equivalent), or (2) seek a warrant and a pen register order concurrently. The search warrant affidavit also must reflect the information noted in the immediately following section of this policy ("Applications for Use of Cell-Site Simulators").

There are two circumstances in which this policy does not require a warrant prior to the use of a cell-site simulator.

1. Exigent Circumstances under the Fourth Amendment

Exigent circumstances can vitiate a Fourth Amendment warrant requirement, but cell-site simulators still require court approval in order to be lawfully deployed. An exigency that excuses the need to obtain a warrant may arise when the needs of law enforcement are so compelling that they render a warrantless search objectively reasonable. When an officer has the requisite probable cause, a variety of types of exigent circumstances may justify dispensing with a warrant. These include the need to protect human life or avert serious injury; the prevention of the imminent destruction of evidence; the hot pursuit of a fleeing felon; or the prevention of escape by a suspect or convicted fugitive from justice.

In this circumstance, the use of a cell-site simulator still must comply with the Pen Register Statute, 18 U.S.C. § 3121, *et seq.*, which ordinarily requires judicial authorization before use of the cell-site simulator, based on the government's certification that the information sought is relevant to an ongoing criminal investigation. In addition, in the subset of exigent situations where circumstances necessitate emergency pen register authority pursuant to 18 U.S.C. § 3125 (or the state equivalent), the emergency must be among those listed in Section 3125: immediate danger of death or serious bodily injury to any person; conspiratorial activities characteristic of organized crime; an immediate threat to a national security interest; or an ongoing attack on a protected computer (as defined in 18 U.S.C. § 1030) that constitutes a crime punishable by a term of imprisonment greater than one year. In addition, the operator must obtain the requisite internal approval to use a pen register before using a cell-site simulator. In order to comply with the terms of this policy and with 18 U.S.C. § 3125,[3] the operator must contact the duty AUSA in the local U.S. Attorney's Office, who will then call the DOJ Command Center to reach a supervisory attorney in the Electronic Surveillance Unit (ESU) of the Office of Enforcement Operations.[4] Assuming the parameters of the statute are met, the ESU attorney will contact a DAAG in the Criminal Division[5] and provide a short briefing. If the DAAG approves, the ESU attorney will relay the verbal authorization to the AUSA, who must also apply for a court order within 48 hours as required by 18 U.S.C. § 3125. Under the provisions of the Pen Register Statute, use under emergency pen-trap authority must end when the information sought is obtained, an application for an order is denied, or 48 hours has passed, whichever comes first.

2. *Exceptional Circumstances Where the Law Does Not Require a Warrant*

There may also be other circumstances in which, although exigent circumstances do not exist, the law does not require a search warrant and circumstances make obtaining a search warrant impracticable. In such cases, which we expect to be very limited, agents must first obtain approval from executive-level personnel at the agency's headquarters and the relevant U.S. Attorney, and then from a Criminal Division DAAG. The Criminal Division shall keep track of the number of times the use of a cell-site simulator is approved under this subsection, as well as the circumstances underlying each such use.

In this circumstance, the use of a cell-site simulator still must comply with the Pen Register Statute, 18 U.S.C. § 3121, *et seq.*, which ordinarily requires judicial authorization before use of the cell-site simulator, based on the government's certification that the information sought is relevant to an ongoing criminal investigation. In addition,

---

[3] Knowing use of a pen register under emergency authorization without applying for a court order within 48 hours is a criminal violation of the Pen Register Statute, pursuant to 18 U.S.C. § 3125(c).

[4] In non-federal cases, the operator must contact the prosecutor and any other applicable points of contact for the state or local jurisdiction.

[5] In requests for emergency pen authority, and for relief under the exceptional circumstances provision, the Criminal Division DAAG will consult as appropriate with a National Security Division DAAG on matters within the National Security Division's purview.

if circumstances necessitate emergency pen register authority, compliance with the provisions outlined in 18 U.S.C. § 3125 is required (see provisions in section 1 directly above).

APPLICATIONS FOR USE OF CELL-SITE SIMULATORS

When making any application to a court, the Department's lawyers and law enforcement officers must, as always, disclose appropriately and accurately the underlying purpose and activities for which an order or authorization is sought. Law enforcement agents must consult with prosecutors[6] in advance of using a cell-site simulator, and applications for the use of a cell-site simulator must include sufficient information to ensure that the courts are aware that the technology may be used.[7]

1. Regardless of the legal authority relied upon, at the time of making an application for use of a cell-site simulator, the application or supporting affidavit should describe in general terms the technique to be employed. The description should indicate that investigators plan to send signals to the cellular phone that will cause it, and non-target phones on the same provider network in close physical proximity, to emit unique identifiers, which will be obtained by the technology, and that investigators will use the information collected to determine information pertaining to the physical location of the target cellular device or to determine the currently unknown identifiers of the target device. If investigators will use the equipment to determine unique identifiers at multiple locations and/or multiple times at the same location, the application should indicate this also.

2. An application or supporting affidavit should inform the court that the target cellular device (*e.g.*, cell phone) and other cellular devices in the area might experience a temporary disruption of service from the service provider. The application may also note, if accurate, that any potential service disruption to non-target devices would be temporary and all operations will be conducted to ensure the minimal amount of interference to non-target devices.

3. An application for the use of a cell-site simulator should inform the court about how law enforcement intends to address deletion of data not associated with the target phone. The application should also indicate that law enforcement will make no affirmative investigative use of any non-target data absent further order of the court, except to identify and distinguish the target device from other devices.

---

[6] While this provision typically will implicate notification to Assistant United States Attorneys, it also extends to state and local prosecutors, where such personnel are engaged in operations involving cell-site simulators.

[7] Courts in certain jurisdictions may require additional technical information regarding the cell-site simulator's operation (*e.g.*, tradecraft, capabilities, limitations or specifications). Sample applications containing such technical information are available from the Computer Crime and Intellectual Property Section (CCIPS) of the Criminal Division. To ensure courts receive appropriate and accurate information regarding the technical information described above, prior to filing an application that deviates from the sample filings, agents or prosecutors must contact CCIPS, which will coordinate with appropriate Department components.

DATA COLLECTION AND DISPOSAL

The Department is committed to ensuring that law enforcement practices concerning the collection or retention[8] of data are lawful, and appropriately respect the important privacy interests of individuals. As part of this commitment, the Department's law enforcement agencies operate in accordance with rules, policies, and laws that control the collection, retention, dissemination, and disposition of records that contain personal identifying information. As with data collected in the course of any investigation, these authorities apply to information collected through the use of a cell-site simulator. Consistent with applicable existing laws and requirements, including any duty to preserve exculpatory evidence,[9] the Department's use of cell-site simulators shall include the following practices:

1. When the equipment is used to locate a known cellular device, all data must be deleted as soon as that device is located, and no less than once daily.

2. When the equipment is used to identify an unknown cellular device, all data must be deleted as soon as the target cellular device is identified, and in any event no less than once every 30 days.

3. Prior to deploying equipment for another mission, the operator must verify that the equipment has been cleared of any previous operational data.

Agencies shall implement an auditing program to ensure that the data is deleted in the manner described above.

STATE AND LOCAL PARTNERS

The Department often works closely with its State and Local law enforcement partners and provides technological assistance under a variety of circumstances. This policy applies to all instances in which Department components use cell-site simulators in support of other Federal agencies and/or State and Local law enforcement agencies.

TRAINING AND COORDINATION, AND ONGOING MANAGEMENT

Accountability is an essential element in maintaining the integrity of our Federal law enforcement agencies. Each law enforcement agency shall provide this policy, and training as appropriate, to all relevant employees. Periodic review of this policy and training shall be the

---

[8] In the context of this policy, the terms "collection" and "retention" are used to address only the unique technical process of identifying dialing, routing, addressing, or signaling information, as described by 18 U.S.C. § 3127(3), emitted by cellular devices. "Collection" means the process by which unique identifier signals are obtained; "retention" refers to the period during which the dialing, routing, addressing, or signaling information is utilized to locate or identify a target device, continuing until the point at which such information is deleted.

[9] It is not likely, given the limited type of data cell-site simulators collect (as discussed above), that exculpatory evidence would be obtained by a cell-site simulator in the course of criminal law enforcement investigations. As in other circumstances, however, to the extent investigators know or have reason to believe that information is exculpatory or impeaching they have a duty to memorialize that information.

responsibility of each agency with respect to the way the equipment is being used (*e.g.*, significant advances in technological capabilities, the kind of data collected, or the manner in which it is collected). We expect that agents will familiarize themselves with this policy and comply with all agency orders concerning the use of this technology.

Each division or district office shall report to its agency headquarters annual records reflecting the total number of times a cell-site simulator is deployed in the jurisdiction; the number of deployments at the request of other agencies, including State or Local law enforcement; and the number of times the technology is deployed in emergency circumstances.

Similarly, it is vital that all appropriate Department attorneys familiarize themselves with the contents of this policy, so that their court filings and disclosures are appropriate and consistent. Model materials will be provided to all United States Attorneys' Offices and litigating components, each of which shall conduct training for their attorneys.

* * *

Cell-site simulator technology significantly enhances the Department's efforts to achieve its public safety and law enforcement objectives. As with other capabilities, the Department must always use the technology in a manner that is consistent with the Constitution and all other legal authorities. This policy provides additional common principles designed to ensure that the Department continues to deploy cell-site simulators in an effective, appropriate, and consistent way.

From: Mayer, Hannah J. \(OPCL\)
Subject: RE: Component overview project
To: Young, Brian A. \(OPCL\); Winn, Peter A. \(OPCL\); Harman-Stokes, Katherine M. \(OPCL\); Ramsden, Michelle \(OPCL\)
Sent: May 9, 2019 3:32 PM (UTC-04:00)
Attached: DAG Rosen Overview Materials CPCLO and OPCL - bay 5-9-19 (HJM).docx

All,

Please find attached my edits and comments. As Brian indicated, the document converted all to author; however, I flagged my edits/comments with my name.

Hannah

From: Young, Brian A. (OPCL) <(b) (6)>
Sent: Thursday, May 09, 2019 9:56 AM
To: Winn, Peter A. (OPCL) <(b) (6)>; Harman-Stokes, Katherine M. (OPCL) <(b) (6)>; Ramsden, Michelle (OPCL) <(b) (6)>; Mayer, Hannah J. (OPCL) <(b) (6)>
Subject: RE: Component overview project

Here are my edits/comments. I'm not sure why Word sometimes just indicates "Author" for who made the Track Changes. It's doing that now. But they're all mine here.

-Brian

Brian A. Young
Senior Counsel
National Security Team Lead
Office of Privacy and Civil Liberties
U.S. Department of Justice
(b) (6) (office)
(b) (6) (mobile)
(202) 307-0693 (fax)
SIPRnet: (b) (6)
JWICS: (b) (6)

From: Winn, Peter A. (OPCL) <(b) (6)>
Sent: Wednesday, May 08, 2019 9:03 PM
To: Harman-Stokes, Katherine M. (OPCL) <(b) (6)>; Young, Brian A. (OPCL) <(b) (6)>; Ramsden, Michelle (OPCL) <(b) (6)>; Mayer, Hannah J. (OPCL) <(b) (6)>
Subject: FW: Component overview project

Jeffrey A. Rosen is expected to be confirmed very shortly as the Deputy Attorney General. Sujit just asked me to prepare an overview of OPCL for incoming DAG Rosen's orientation package. Can each of you please review the attachment which we prepared for AG Barr in February, and send me any edits or comments you have by COB tomorrow?

Peter

From: Ramsden, Michelle \(OPCL\)
Subject: RE: Component overview project
To: Mayer, Hannah J. \(OPCL\); Young, Brian A. \(OPCL\); Winn, Peter A. \(OPCL\); Harman-Stokes, Katherine M. \(OPCL\)
Sent: May 9, 2019 3:47 PM (UTC-04:00)
Attached: DAG Rosen Overview Materials CPCLO and OPCL - bay 5-9-19 (HJM)(AMR).docx

Thanks Hannah for making some good points which I shamelessly piggybacked on to.

Michelle Ramsden
Attorney Advisor
Office of Privacy & Civil Liberties
U.S. Department of Justice
2 Constitution Square, 8W.703
145 N St. NE
Washington, D.C. 20002
Desk: (b) (6)
Mobile: (b) (6)
E-mail: (b) (6)

From: Mayer, Hannah J. (OPCL) <(b) (6)>
Sent: Thursday, May 9, 2019 3:32 PM
To: Young, Brian A. (OPCL) <(b) (6)>; Winn, Peter A. (OPCL) <(b) (6)>; Harman-Stokes, Katherine M. (OPCL) <(b) (6)>; Ramsden, Michelle (OPCL) <(b) (6)>
Subject: RE: Component overview project

Duplicative Information - See Document ID 0.7.12327.16401

From: Harman-Stokes, Katherine M. \(OPCL\)
Subject: RE: Component overview project
To: Ramsden, Michelle \(OPCL\); Mayer, Hannah J. \(OPCL\); Young, Brian A. \(OPCL\); Winn, Peter A. \(OPCL\)
Sent: May 9, 2019 5:13 PM (UTC-04:00)
Attached: 2019-5-9 - DAG Rosen Overview Materials CPCLO and OPCL - bay 5-9-19 (HJM)(AMR) (khs).docx

I've updated more. Peter, back to you.
Thanks everyone!
Kathy

From: Ramsden, Michelle (OPCL) <(b) (6) >
Sent: Thursday, May 9, 2019 3:47 PM
To: Mayer, Hannah J. (OPCL) <(b) (6) >; Young, Brian A. (OPCL) <(b) (6) >; Winn, Peter A. (OPCL) <(b) (6) >; Harman-Stokes, Katherine M. (OPCL) <(b) (6) >
Subject: RE: Component overview project

Duplicative Information - See Document ID 0.7.12327.13302

From: Winn, Peter A. \(OPCL\)
Subject: OPCL Overview Materials for DAG Rosen
To: Robinson-Smith, Andria \(OPCL\)
Cc: Harman-Stokes, Katherine M. \(OPCL\)
Sent: May 10, 2019 9:27 AM (UTC-04:00)
Attached: 2019-5-9 - DAG Rosen Overview Materials CPCLO and OPCL PAW Edits.docx

Andria,

Here is the version to incorporate into the new format.

Thanks.
Peter

Peter A. Winn
Acting Chief Privacy and Civil Liberties Officer
United States Department of Justice
Office of Privacy and Civil Liberties
Two Constitution Square (2CON)
145 N Street, NE
Suite 8W.300
Washington DC 20530
Office (b) (6)
Cell (b) (6)
Fax (202) 307-0693
(b) (6)
(b) (6)
(b) (6)
https://www.justice.gov/opcl

M E M O R A N D U M

To: Deputy Attorney General Jeffrey A. Rosen

From: Peter A. Winn, Acting Chief Privacy and Civil Liberties Officer

Date: May 10, 2019

Subject: Chief Privacy and Civil Liberties Officer and the Office of Privacy and Civil Liberties Overview for Deputy Attorney General Rosen

---

I. ABOUT THE CHIEF PRIVACY AND CIVIL LIBERTIES OFFICER AND THE OFFICE OF PRIVACY AND CIVIL LIBERTIES

Background

As part of the body of legislation enacted following the September 11, 2001 attacks, Congress established the position of Chief Privacy and Civil Liberties Officer ("CPCLO") as the senior official primarily responsible for the Department's privacy and civil liberties compliance and policy.[1] The 9/11 Commission had noted that the government would need to access vast amounts of personal data in carrying out its law enforcement and national security missions. It accordingly recommended that Congress establish CPCLOs at critical agencies in the antiterrorist fight to maintain the trust of the American people in the government's ability to carry out its law enforcement and national security mission lawfully and appropriately.[2] After consolidating Department of Justice privacy compliance and advice responsibilities under the

[1] Implementing Recommendations of the 9/11 Commission Act of 2007, P.L. 110-53, § 803, 121 Stat. 299, 360 (Aug. 3, 2006) (codified at 42 U.S.C. § 2000ee-1) (Requiring designation of a senior official to be responsible for privacy policy, including advising the head of the agency with respect to the privacy and civil liberties implications of any proposed or existing laws, regulations, procedures and guidelines, particularly when these relate to efforts to protect the Nation against terrorism, and addressing complaints relating to these concerns). Before the 2006 and 2007 statutory changes consolidated the Department's compliance and policy functions within the CPCLO, privacy compliance issues were the responsibility of the Office of Privacy and Information Policy (OPIP), while an Associate Deputy Attorney General with the title of Chief Privacy Officer addressed important privacy policy concerns. Because Congress mandated that the CPCLO was to report directly to the head of the agency, the CPCLO continued to sit as a senior member of the Deputy Attorney General's staff to ensure effective agency-wide oversight. *See also* Violence Against Women Act and Department of Justice Reauthorization Act of 2005, P.L. 109-162, § 1174, 119 Stat. 2960, 3124 (Jan. 5, 2006) (codified at 28 U.S.C. § 509, note) (Requiring the Attorney General to designate a senior official to assume primary responsibility for privacy policy, including ensuring appropriate privacy protections are established and maintained for existing and proposed new information technologies, reviewing legislative and regulatory proposals, implementing policies and procedures and providing appropriate training to ensure the Department's compliance with federal privacy laws and policy).

[2] THE 9/11 COMMISSION REPORT: FINAL REPORT OF THE NATIONAL COMMISSION ON TERRORIST ATTACKS UPON THE UNITED STATES, at 395 (2004).

CPCLO pursuant to these laws, the Department created the Office of Privacy and Civil Liberties ("OPCL") to support the work of the CPCLO.[3]

Mission

The principal mission of OPCL is to protect the privacy and civil liberties of the American people through review, oversight, and coordination of the Department's privacy operations. OPCL provides legal advice and guidance to all 42 Departmental components; ensures the Department's privacy compliance; develops and provides Departmental privacy training; assists the CPCLO in developing Departmental privacy policy; prepares privacy-related reporting to the President and Congress; and reviews the information handling practices of the Department to ensure that such practices are consistent with the protection of privacy and civil liberties.

OPCL is responsible for ensuring that all of the Department's components comply with the Privacy Act of 1974, as amended ("Privacy Act"), the E-Government Act of 2002 ("E-Government Act"), the Federal Information Security Modernization Act of 2014 ("FISMA"), as well as a number of other statutes and administration policy directives. OPCL handles questions of legal interpretation regarding these laws, and reviews and approves the Department's Privacy Act filings with the *Federal Register*, as well as Privacy Impact Assessments and related documentation required under the E-Government Act. OPCL also trains Department employees about their responsibilities under these privacy laws and directives, and prepares privacy-related reports to the President and Congress. Because privacy and cybersecurity overlap on protecting personal information, OPCL works closely with the Office of the Chief Information Officer ("OCIO") to ensure that the privacy compliance requirements for which OPCL is responsible dovetail with OCIO's efforts to protect the security of the Department's information systems. These offices also work jointly to respond to data breaches, and manage risks associated with the design and operation of the Department's information systems. In general, OPCL's compliance mission is to ensure that the Department manages sensitive personal information lawfully and appropriately, and maintains public trust in its ability to carry out its mission in an age of electronic information.

The CPCLO's policy mission includes advising DOJ leadership and components, and working as part of interagency groups on novel questions of privacy law and policy. This includes reviewing proposed legislation and regulations to identify and address privacy-related concerns; supporting the Department in privacy-related litigation; periodically updating the Attorney General's Guidelines for the handling of information concerning United States persons under Sections 2.3 and 2.4 of Executive Order 12333 (in coordination with the National Security Division, the Federal Bureau of Investigation (FBI), the Office of the Director of National Intelligence, and the respective intelligence agency); serving on the Federal Privacy Council and

[3] The Department created OPCL by moving the privacy specialists from what was then OPIP, to a newly created OPCL, and renaming OPIP as the Office of Information Policy (OIP). OIP now focuses exclusively on access requests under the FOIA and Privacy Act.

a number of interagency privacy and civil liberties working groups to mitigate privacy risks involved in the use of personal data in the government's efforts to protect the Nation against terrorism; and participating in a number of other law enforcement and national security advisory committees and working groups. The CPCLO and OPCL staff are also responsible for conducting outreach to stakeholders in industry, academic and civil society organizations to insure better understanding of the Department's privacy programs and policies.

The CPCLO also plays an increasing role defending U.S. national security and law enforcement data handling practices, and the U.S. privacy system, against legal challenges and other official actions by overseas data protection authorities (mostly in the European Union), privacy advocates, the United Nations, and international organizations. OPCL works to advance DOJ's interests in U.S. and international legislative, regulatory, and policy initiatives designed to strengthen privacy safeguards and/or coordinate privacy legal regimes. Here OPCL works with the Office of Legal Policy (OLP) and other DOJ components to support the U.S. Department of State to prepare the USG's response to various United Nations privacy-related efforts, including reviews by the UN Human Rights Committee's Special Rapporteur for the Right to Privacy, meetings of the Secretary-General's High-level Panel on Digital Cooperation, and proposed UN resolutions such as the Resolution on Privacy in the Digital Age. OPCL also arranges meetings between foreign government privacy officials and DOJ components to help the foreign officials better understand the USG's law enforcement and national security privacy safeguards.

II. GENERAL BACKGROUND

Location

Office of Privacy and Civil Liberties
Two Constitution Square (2CON)
145 N Street, NE, Suite 8W.300
Washington, DC 20002

Website

https://www.justice.gov/opcl

Component Structure

The CPCLO is designated by the Attorney General and reports to the Deputy Attorney General. Since January 2017, Peter Winn, the Director of OPCL, a career official in the Senior Executive Service, has served as the Acting CPCLO. OPCL is staffed by a Director and a Deputy Director, who oversee a staff of four attorneys, one Privacy Analyst and one Program Specialist. As funding permits, OPLC also has two attorney contractors and one contractor who performs administrative duties. OPCL staff work with Senior Component Officials for Privacy (SCOPs) within each of the Department's components, which, depending on their size, may

oversee a team of privacy specialists (e.g., the FBI), while others (e.g., OLC), may perform their SCOP duties on only a part-time basis.

Total Number of Personnel

1	Department CPCLO (Acting); Director, OPCL
1	Deputy Director, OPCL
4	Attorney Advisors
1	Privacy Analyst
1	Program Specialist
2	Contractor - Attorneys (as funding permits)
1	Contractor - Privacy Analyst/Administrative support (as funding permits)
11	**Total**

Key Personnel

TITLE	NAME	CONTACT INFORMATION
Acting Department CPCLO, Director of OPCL	Peter A. Winn	(b) (6)
Deputy Director	Katherine Harman-Stokes	(b) (6)

Acting Chief Privacy and Civil Liberties Officer, Director OPCL

Since January 20, 2017, Peter Winn, the Director of OPCL, has served as Acting CPCLO of the Department. Winn has been with the Department since 1994, where he has also served as an AUSA and an Attorney-Advisor in the Office of Legal Counsel. He served a detail as the acting General Counsel to the Privacy and Civil Liberties Oversight Board during its review of the NSA programs that were the subject of unauthorized disclosures by Edward Snowden. Before joining DOJ, Winn was a Special Assistant Attorney General for the Attorney General of Texas, and an associate at Patterson Belknap Webb and Tyler in New York City, where he worked for former DAG Harold Tyler and the future Attorney General Michael Mukasey. He clerked for James B. McMillan in the Western District of North Carolina. Winn also has taught part-time at the University of Washington, Southern Methodist University, and the University of Melbourne, has published articles on the Fourth Amendment, computer security, health privacy, and the right of public access to court records. He received his J.D. *cum laude* from Harvard Law School, an MPhil in Philosophy from the University of London (where he was a Marshall Scholar), and a B.A. *magna cum laude* from Williams College.

III. CRITICAL CASES AND ISSUES

1. Access by government law enforcement, national security, and regulatory agencies to consumer data on platforms and equipment controlled by large multi-national technology companies will continue to be subject to legal and policy challenges based on privacy and civil liberties concerns.
   a. Domestically, there is a much greater likelihood than in the past of federal legislation creating a national domestic privacy law for consumer data. OPCL has focused on making sure that any such legislation does not limit lawful and appropriate use of personal information for law enforcement, national security, and regulatory purposes.
   b. Data platforms run by American technology companies are increasingly transnational, making these companies the subject of overseas legal and regulatory challenges based on foreign privacy laws due to the U.S. companies' compliance with lawful demands by U.S. government agencies for access to personal data for law enforcement, national security and regulatory purposes. These challenges have reached a critical pitch in the European Union, because of opinions by the European Court of Justice and by regulatory actions by the European Commission and Parliament. The challenges are increasing through various United Nations activities as well, as discussed above. Congress has attempted to address some of these concerns by enacting the Judicial Redress Act and the Clarifying Lawful Overseas Use of Data Act ("CLOUD Act"), and the U.S. Government has entered into international arrangements like the Privacy Shield and the Data Privacy and Protection Agreement with the European Union. OPCL devotes substantial resources to address an ever-growing range of international privacy-related concerns, working with various USG teams to meet with authorities from the European Union, Canada, Australia, New Zealand, and other countries.

2. Terrorist watchlisting, NSPM-7 (Integration, Sharing, and Use of National Security Threat Actor Information to Protect Americans), and NSPM-9 (Optimizing the Use of Federal Government Information in Support of the National Vetting Enterprise) involve large and controversial information-sharing programs designed to allow national security and law enforcement agencies to access, use, and disseminate large volumes of personal information. OPCL has devoted substantial resources to helping ensure that these law enforcement and national security information-sharing programs operate lawfully and appropriately. Because such programs are frequently the subject of judicial challenges, OPCL works to create and maintain strong ex-ante compliance structures, and works closely with the Department's litigators when these programs are challenged.

3. As the Department has increasingly relied on new information systems and technologies, its privacy compliance responsibilities have continued to increase as well. OPCL's limited resources and component privacy teams have not increased accordingly, and a (b) (5)

(b) (5) [redacted]

4. Following is a non-exhaustive list of additional privacy and civil liberties matters OPCL is responsible for or significantly involved in:
   a. The Department's Breach Response Plan and implementation of DOJ Instruction 0900.0.01
   b. Implementation of policies, procedures, and reviews for compliance with OMB Circular A-130, NIST Spec. Pub. 800-53, Rev. 4, Appendix J Privacy Controls, and NIST frameworks
   c. Open Government
   d. Insider Threat Working Group
   e. Privacy Legislation Small Group
   f. Forensic Genealogy Working Group
   g. Social Media Working Group
   h. Mandatory Training Advisory Group
   i. Learning Development Council
   j. Information Sharing Environment (ISE)
   k. Special Operations Review Committee (SORC)
   l. National Domestic Communications Assistance Center (NDCAC)
   m. Global Advisory Committee
   n. Unmanned Aerial Surveillance (UAS) and Counter--UAS
   o. Cell site simulators
   p. Cybersecurity Information Sharing Act (CISA), CISA Reports, and cybersecurity matters
   q. Social Media, websites, mobile, and digital services
   r. Judicial Redress Act
   s. Privacy Shield
   t. United Nations resolutions
   u. International data protection

v. International litigation
w. Privacy Act and privacy-related litigation support
x. Privacy Act Overview
y. Legislative Affairs and Policy reviews
z. GAO Audit privacy reviews
aa. OIG investigation summary reviews
bb. Federal Information Security Modernization Act Report
cc. Data Mining Report
dd. Executive Order 13636 Report
ee. Section 803 Reports
ff. CPCLO Annual Report
gg. SSN Reduction Act Report
hh. U.S. State Department International Leadership Visitors Program
ii. Department-wide Privacy Act training and awareness