ELECTRONIC COMMUNICATIONS SURVEILLANCE: WHAT JOURNALISTS AND MEDIA ORGANIZATIONS NEED TO KNOW

Jennifer R. Henrichsen and Hannah Bloch-Wehba[*]

[*] Henrichsen is a Ph.D. student at the University of Pennsylvania's Annenberg School for Communication and a former First Look Media Technology Fellow at the Reporters Committee. Bloch-Wehba is Stanton First Amendment Fellow, Associate Research Scholar in Law and Clinical Lecturer in Law at Yale Law School and a former Stanton Foundation National Security Fellow at the Reporters Committee. With deep gratitude, the Reporters Committee thank First Look Media and the Stanton Foundation for their support for this project. The authors are indebted to Selina MacLaren for her careful and thorough assistance in getting this project to its final form.

I. INTRODUCTION

The practice of journalism has never been more global than it is today. Reporters use Skype, Google Hangout, and other video chat services to communicate with sources halfway around the world. Newsrooms rely on cloud storage to share documents among far-flung teams working on global stories. Individuals and organizations increasingly turn to cutting-edge technologies to break important news.

At the same time, new applications and services can pose risks to the security and integrity of communications. Journalists and news media organizations have increasingly been the targets of hacking. Edward Snowden's revelations brought to the fore the broad reach of U.S. surveillance programs both domestically and abroad. And while the Department of Justice has strengthened its internal guidelines governing the use of legal process to obtain information from, or records of, the news media, *see* 28 C.F.R. § 50.10, some details about the implementation of those reforms remain unclear, despite the urging of press advocates.[1]

Responding to the shift from the analog world to the world of electronic communications, national security apparatuses like the National Security Agency have developed programs to collect, analyze, and retain these communications. Sometimes these programs sweep up data from a large number of Americans in bulk, either purposefully or as a result of "incidental" acquisitions obtained while surveilling individual targets of an investigation. Bulk surveillance of communications—whether collected "incidentally" under Section 702 of the FISA Amendments Act of 2008,[2] through the procedures set out in the amended Section 215 program,[3] or under Executive Order 12333[4]—implicates reporters' rights in myriad ways. These programs may collect information that can reveal details of confidential communications between reporters and their sources. Because this information is not always gleaned directly from reporters, however, journalists are uncertain about the extent to which their communications are exposed. The inability to know whether and to what extent communications are being monitored creates fear and uncertainty concerning what the government considers lawful surveillance, chills speech, and impedes the exercise of First Amendment rights, including free association and free expression.

Both journalists and sources have stated that bulk surveillance and increased leak investigations make them more reluctant to communicate with each other, even if the information at issue is not classified.[5] The "chilling effect" of mass surveillance has been documented in several reports by organizations including PEN America, Human Rights Watch, and the American Civil Liberties Union, among others.[6]

---

[1] For example, the guidelines' application to administrative subpoenas remains ambiguous.
[2] 50 U.S.C. § 1881a.
[3] 50 U.S.C. § 1861.
[4] Executive Order 12333.
[5] Leonard Downie Jr., *Leak investigations and surveillance in post 9-11 America,* Committee to Protect Journalists (Oct. 10, 2013), *available at* https://cpj.org/reports/2013/10/obama-and-the-press-us-leaks-surveillance-post-911.php.
[6] PEN America, *Global Chilling: The Impact of Mass Surveillance on International Writers* (Jan. 5, 2014), *available at* http://www.pen.org/global-chill; *see also*, Human Rights Watch and ACLU, *With Liberty To Monitor All: How Large-Scale US Surveillance is Harming Journalism, Law and American Democracy* (2014), *available at* https://www.hrw.org/sites/default/files/reports/usnsa0714_ForUPload_0.pdf.

But bulk surveillance is not the only threat; other national security requests have also been directed at journalists without a warrant. Even apart from NSA surveillance, it has never been easier for governments to obtain information about private communications, including the emails, phone calls, messaging logs, and browsing histories of journalists and sources. The ability of governments, corporations, and other non-state actors to obtain information, target searches, and store vast amounts of data for indeterminate periods of time poses a threat to the traditional journalist-source relationship, especially when a source seeks to remain anonymous. Government agencies, other than the Justice Department, have not disclosed the policies and procedures, if any, they use to ensure that surveillance does not tread on the First Amendment rights of journalists and media organizations. Nonetheless, the potential use of national security surveillance to reveal reporters' confidential sources and open the newsgathering process to government scrutiny poses a real threat to the freedom of the press.

The behavior of journalists and sources adds to the challenge. Both communities are often unaware of the risks of communicating electronically, or if they are aware of the risks, they may not know how to determine what steps are necessary to protect their communications. Email encryption, secure messaging, and anonymous web-browsing can be helpful tools, but can also be difficult to implement.

This guide has two aims. First, in light of the Justice Department's revised news media guidelines, we attempt to clarify the scope of U.S. government authority to obtain information about journalists' communications. The new guidelines were a welcome development, but the Justice Department did not hide the fact that they did not apply to all forms of legal process that could be used against the press. U.S. surveillance law is complex and wide-ranging, so this guide necessarily offers only an overview of the main statutes, including not only the laws underpinning some of the now well-known NSA surveillance programs, but also other statutes authorizing the government to conduct communications surveillance in the foreign intelligence, national security, and criminal justice settings. In some cases, the laws are covered by the guidelines; in other cases, they are not.

Second, we outline how some common journalism tools expose reporters and sources to risks in light of this framework. It is our hope that a better understanding of the legal architecture that facilitates government access to communications records will help journalists make informed decisions about the types of security tools they use.

Finally, the annual reporting the Justice Department has undertaken under the new 50.10 guidelines[7] means that the public has at least some information about the frequency of legal demands for press records. For example, the Justice Department reported in its "Annual Report: Calendar Year 2014" that the Attorney General authorized subpoenas, court orders, and search warrants for information from or records of the news media three times, including one

[7] *See* Dep't of Justice, Annual Report: Use of Certain Law Enforcement Tools to Obtain Information from, or Records of, Members of the News Media; and Questioning, Arresting, or Charging Members of the News Media, 1 (2015) (noting that a Feb. 21, 2014 Attorney General Memorandum committing the Attorney General to make public, on an annual basis, data regarding the Department's use of certain law enforcement tools to obtain information from, or records of, members of the news media, and regarding questioning, arresting, or charging members of the news media, pursuant to 28 C.F.R. § 50.10); *see also* United States Attorneys' Manual (USAM) 9-13.400(L)(4).

application for a search warrant in connection with a hacking investigation.[8] The Justice Department reported one case in its "Annual Report: Calendar Year 2015" in which the Attorney General authorized such a search for information of the news media; two cases in which the Deputy Assistant Attorney General for the Criminal Division authorized such searches; and 22 cases in which Assistant Attorneys General or U.S. Attorneys authorized subpoenas and applications for court order for information from the news media.[9] For the tools identified in this report to which the guidelines do not apply, we are aware of only this: the government has ways to conduct investigations without triggering the guidelines' requirements of authorization and notice.

II. LEGAL AND REGULATORY PROTECTIONS FOR JOURNALISTS

In the United States, journalists have constitutional, statutory, common law, and regulatory protections that help ensure their ability to gather and report the news without government interference. Two of the most important legal protections available to U.S. journalists include the First Amendment and state shield laws. In the regulatory sphere, the aforementioned updated protections in Justice Department guidelines require the government to meet certain conditions before using common investigative tools to obtain records belonging to or relating to journalists.[10]

A. Constitutional protection: The First and Fourth Amendments.

The First Amendment to the U.S. Constitution guarantees freedom of expression by, among other things, prohibiting any law that infringes the freedom of the press, or the rights of individuals to speak freely. The First Amendment affords broad protection to journalists and news organizations engaged in the gathering and dissemination of news, and a core purpose of the First Amendment is the fostering of robust and uninhibited debate on public issues.[11] For example, in *Bartnicki v. Vopper*,[12] the U.S. Supreme Court held that the First Amendment protected a news organization from liability for the publication of information of public interest that had been obtained unlawfully by a source. The use of subpoenas to compel journalists to identify sources also presents serious First Amendment concerns: Several federal circuits have recognized a qualified reporters' privilege under the First Amendment in both civil and criminal cases to protect journalists from compelled disclosure of their sources.[13]

---

[8] Dep't of Justice, Annual Report: Use of Certain Law Enforcement Tools to Obtain Information from, or Records of, Members of the News Media; and Questioning, Arresting, or Charging Members of the News Media (2014) at 2, *available at* https://www.justice.gov/criminal/file/760981/download.

[9] *See generally* Dep't of Justice, Annual Report: Use of Certain Law Enforcement Tools to Obtain Information from, or Records of, Members of the News Media; and Questioning, Arresting, or Charging Members of the News Media (2015), *available at* https://www.justice.gov/criminal/file/888316/download.

[10] *See generally* 28 C.F.R. § 50.10 (discussed *infra* at 7).

[11] RCFP's First Amendment Handbook provides a primer on how the First Amendment protects journalists in a range of contexts, including from libel and defamation charges, privacy torts, and prior restraints. *See* Reporters Committee for Freedom of the Press, *First Amendment Handbook*, *available at* https://www.rcfp.org/first-amendment-handbook; *see also* Reporters Committee for Freedom of the Press, *Digital Journalists Legal Guide*, *available at* https://www.rcfp.org/digital-journalists-legal-guide/sources-and-subpoenas-reporters-privilege.

[12] 532 U.S. 514 (2001).

[13] *See, e.g.*, *von Bulow by Auersperg v. von Bulow*, 811 F.2d 136, 142 (2d Cir. 1987) (reasoning that "the process of newsgathering is a protected right under the First Amendment, albeit a qualified one," and that "[t]his qualified right . . . results in the journalist's privilege"); *Miller v. Transamerican Press, Inc.*, 621 F.2d 721, 725 (5th Cir. 1980) (recognizing a qualified privilege not to disclose confidential informants in civil cases); *United States v. LaRouche*

Along with First Amendment protections, Fourth Amendment protections are among the most crucial constitutional safeguards of newsgathering in the context of government investigations. The Fourth Amendment provides that "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause."[14] The prohibition on unreasonable searches of "papers" and the use of "general warrants" arose from a long list of abusive colonial-era practices, many of which targeted printers and publishers of dissenting publications for seditious libel.

Under the Fourth Amendment, a "search" occurs only when the person searched has a "reasonable expectation of privacy" in the place or thing to be searched.[15] What a person "knowingly discloses" to a third party is not the subject of Fourth Amendment protections, and government requests for such information do not require a warrant or probable cause. As a result, because a telephone subscriber "knowingly discloses" dialed numbers to the telephone company, courts have held that the use of a subpoena or court order to obtain that information does not implicate the Fourth Amendment.[16] In several pending challenges to the constitutionality of the government's bulk collection of telephony metadata, discussed in more detail below, plaintiffs have challenged the application of this "third party doctrine" to large-scale collection activity.

The third party doctrine has significant ramifications for the protection of electronic communications. For example, electronic communications service providers necessarily have access to metadata such as telephone numbers, email to/from addresses, IP addresses of websites visited, and other addressing data that users are aware "is provided to and used by Internet service providers for the specific purpose of directing the routing of information."[17] This metadata can be obtained through many types of legal process. On the other hand, although the content of emails, instant messages, and text messages are often accessible by service providers as well, courts that have addressed the issue have found that individuals retain a reasonable expectation of privacy in the substance of their communications.[18] As a result, the government may *not* obtain the content without a search warrant.[19]

But as a practical matter, many surveillance authorities permit the government to obtain information that law enforcement can use to identify sources without using formal process such as subpoenas or warrants, compelling testimony, or giving notice to a journalist whose communications may be secretly monitored or seized. Reporters whose records are obtained

---

Campaign, 841 F. 2d 1176, 1181–83 (1st Cir. 1988). For more information, *see* Reporters Committee for Freedom of the Press, *The Reporters Privilege*, *available at* https://rcfp.org/reporters-privilege.

[14] U.S. Const. Amend. IV.

[15] *Katz v. United States*, 389 U.S. 347, 360 (1967) (Harlan, J., concurring).

[16] *See, e.g., Smith v. Maryland*, 442 U.S. 735, 741–46 (1979).

[17] *United States v. Forrester*, 512 F.3d 500, 510 (9th Cir. 2008).

[18] *See, e.g.*, *United States v. Warshak*, 631 F.3d 266, 288 (6th Cir. 2010); *Forrester*, 512 F.3d at 511; *cf. United States v. Hambrick*, 225 F.3d 656, 2000 WL 1062039, at *2 (4th Cir. 2000) (per curiam) (finding no reasonable expectation of privacy in non-content information provided to an ISP). *See also* Orin S. Kerr, *The Next Generation Communications Privacy Act*, 162 U. Pa. L. Rev. 373, 399–400 (2014) (noting that "several lower courts have ruled that the Fourth Amendment fully protects the contents of emails held by third party providers" and "*Warshak* has been adopted by every court that has squarely decided the question").

[19] To the extent the Stored Communications Act appears to permit warrantless acquisition of content data, it violates the Fourth Amendment. *See, e.g., Warshak*, 631 F.3d at 288.

pursuant to national security processes such as National Security Letters, directives or orders under the Foreign Intelligence Surveillance Act (FISA), or delayed-notice warrants or subpoenas would almost certainly not be notified or have an opportunity to try to quash the request. Indeed, reporters may not even be aware that national security processes have been used to obtain their records. This uncertainty has been an impediment to journalists wishing to challenge surveillance practices that impact their own newsgathering processes.[20]

In the national security context, the Fourth Amendment's application is complex. The Fourth Amendment's protections apply domestically, and to U.S. persons abroad, but do not apply to non-citizens abroad.[21] There are no protections under the U.S. Constitution for non-citizens abroad who are affected by foreign intelligence investigations. As a result, surveillance of non-U.S. persons abroad is outside the scope of the Fourth Amendment. However, because some of the surveillance authorities used to collect the communications of non-U.S. persons abroad sweep up many communications belonging to U.S. persons as well, courts have considered whether those programs are "reasonable" under the Fourth Amendment.[22]

B. Statutory and common law protections: state shield laws, testimonial privileges, and the Privacy Protection Act.

The majority of states recognize a reporter's privilege based on state law.[23] Thirty-nine states and the District of Columbia have shield laws, which give media varying degrees of protection for confidential source information.[24] Some shield laws protect reporters from forced disclosure of their sources. Other shield laws provide qualified or absolute protection that varies depending on the type of legal proceeding (civil or criminal), the scope of the statute's definition of "journalists," whether material is confidential and/or published, and whether the journalist is a defendant or an independent third party. No federal shield law exists, despite several efforts to enact such statutory protections by legislators at the national level.[25] In addition, some judges have argued that federal common law establishes a qualified reporter's privilege in certain settings.[26]

---

[20] *See, e.g.*, ACLU v. NSA, 493 F. 3d 644, 662–65 (6th Cir. 2007) (noting that the journalists' injury involved "purely speculative fears" and a "personal subjective chill" that was not sufficiently concrete, actual, or imminent to establish standing for a First Amendment cause of action).

[21] *See United States v. Verdugo-Urquidez*, 494 U.S. 259, 274–75 (1990) (holding that Fourth Amendment did not apply to a citizen and resident of Mexico where the search occurred in Mexico).

[22] *See* Mem. Op. and Order at *28–29, FISC (Oct. 3, 2011) (J. Bates), *available at* http://www.dni.gov/files/documents/0716/October-2011-Bates-Opinion-and%20Order-20140716.pdf.

[23] *See, e.g.*, *O'Neill v. Oakgrove Construction Inc*., 71 N.Y.2d 521, 524 (1988) (recognizing a reporter's privilege under state constitution).

[24] Alabama, Alaska, Arizona, Arkansas, California, Colorado, Connecticut, Delaware, Florida, Georgia, Hawaii, Illinois, Indiana, Kansas, Kentucky, Louisiana, Maine, Maryland, Michigan, Minnesota, Montana, Nebraska, Nevada, New Jersey, New York, North Carolina, North Dakota, Ohio, Oklahoma, Oregon, Pennsylvania, Rhode Island, South Carolina, Tennessee, Texas, Washington, and Wisconsin all have shield statutes. In addition, certain courts recognize a common law privilege. Finally, New Mexico and Utah courts recognize a privilege through court rules.

[25] *See* Reporters Committee for Freedom of the Press, *Shield laws and protection of sources by state, available at* https://www.rcfp.org/browse-media-law-resources/guides/reporters-privilege/shield-laws.

[26] *See, e.g.*, *Riley v. City of Chester*, 612 F.2d 708 (3d Cir. 1979) (concluding that "journalists have a federal common law privilege, albeit qualified, to refuse to divulge their sources" outside the grand jury setting); *In re Grand Jury Subpoena Miller*, 397 F.3d 964 (D.C. Cir. 2005) (J. Tatel, concurring), *opinion superseded by* 438 F.3d 1141 (D.C. Cir. 2006); *New York Times Co. v. Gonzales*, 459 F.3d 160 (2d Cir. 2006) (Sack, J., dissenting).

In recognition of the importance of safeguarding journalists and newsrooms from improper searches and seizures by law enforcement, federal law offers additional protections from searches and seizures beyond those afforded by the First and Fourth Amendments. The Privacy Protection Act of 1980 ("PPA")[27] prohibits searches for certain types of materials related to newsgathering and publishing activities, except under limited circumstances. Generally speaking, the PPA prevents the government from searching or seizing work product or documentary materials possessed by a person "in connection with a purpose to disseminate to the public a newspaper, book, broadcast, or other similar form of public communication" unless there is probable cause to believe that the person has committed or is committing a criminal offense related to the materials.[28]

The PPA's coverage is limited, however, in part because the statute explicitly permits the government to search for work product or documentary materials when the possessor is suspected of violating the Espionage Act.[29] Under the guidelines, this "suspect exception" can be invoked where the news media or member of the news media is the focus of the criminal investigation for conduct that goes beyond ordinary new-gathering activities.[30] The PPA also permits the government to search for work product or documentary materials if there is reason to believe that the immediate seizure of the materials is necessary to prevent death or serious bodily injury to any human being, and further permits searches of documentary materials if there is reason to believe that issuing a subpoena would result in the destruction, alteration, or concealment of such materials.[31] As such, the PPA goes a step beyond the Fourth Amendment in granting additional protections to journalists' work product and documentary materials, but still provides considerable latitude to government investigators, particularly in the context of national security investigations.

C. Regulatory protection: The Department of Justice's media subpoena and search warrant guidelines.

As mentioned earlier, the Department of Justice has issued guidelines governing the use of certain law enforcement tools to obtain records of or pertaining to the news media.[32] Prior to 2014, the guidelines covered subpoenas; today, they cover search warrants, subpoenas, and court orders issued under the Stored Communications Act.[33] The guidelines are not legally enforceable but might be considered a "social contract" between the news media and the government.

Generally speaking, the guidelines require the Attorney General to authorize the Department to use a subpoena or warrant to obtain records, including communications records,

---

[27] 42 U.S.C. § 2000aa *et seq*.
[28] *Id*. at § 2000aa(a), (b). The suspected criminal offense must be something other than merely receiving, possessing, communicating, or withholding the materials, unless, however, the offense concerns national security or child pornography, in which case an offense of receipt or possession may be enough to permit a search.
[29] *Id.* at § 2000aa(a)(1) ("[S]uch a search or seizure may be conducted under the provisions of this paragraph if the offense consists of the receipt, possession, or communication of information relating to the national defense, classified information, or restricted data . . .").
[30] *See* Department of Justice Report on Review of News Media Policies, 3 (Jul. 12, 2013), *available at* https://www.justice.gov/sites/default/files/ag/legacy/2013/07/15/news-media.pdf.
[31] 42 U.S.C. § 2000aa(a)(2); 2000aa(b)(2); 2000aa(b)(3).
[32] 28 C.F.R. § 50.10.
[33] *Id*.

of a member of the news media.[34] The guidelines' coverage of subpoenas extends beyond grand jury and trial subpoenas to administrative subpoenas issued by the Department and its components, except for National Security Letters, discussed below.[35] In addition, Department of Justice attorneys must "consult with the Criminal Division" before moving to enforce subpoenas, warrants, or court orders sought by other agencies.[36] However, agencies other than the Department of Justice are not bound by the guidelines when they make any initial demands on the press.

The guidelines generally require that the Department seek information from a member of the news media only when it is "essential," after the Department has sought the information from alternative sources, and after the Department has undertaken negotiations with the affected member of the news media. When a member of the news media is the "subject or target of an investigation relating to an offense committed in the course of, or arising out of, newsgathering activities," however, the Department need not seek the same information from alternative sources nor negotiate with the affected member of the news media. The guidelines also do not apply to information sought from journalists that is unrelated to newsgathering. Finally, as discussed below, the guidelines do not apply to communications or other records obtained through FISA court orders, bulk surveillance, or other national security processes.[37]

III. ELECTRONIC COMMUNICATIONS SURVEILLANCE AUTHORITIES

Journalists in the U.S. face numerous challenges when striving to protect their sources. These challenges include, but are not limited to, collection and interception of communications by the U.S. government and prosecutors' aggressive pursuit of sources for government leaks. Combined, these factors greatly challenge journalists' ability to communicate securely with sources, assure sensitive sources that the communications will be confidential, and gather news vital to the public interest.

There are a number of reasons reporters might be concerned about the scope of "surveillance authority"—our shorthand term for a variety of statutes that enable the government to request and obtain information about stored or real-time communications. Government agents may use surveillance authority to gain access to the content of reporters' communications, as well as to obtain certain records related to those communications. For example, agents might use a trap and trace order to obtain a list of telephone numbers dialed by the reporter, or use a National Security Letter to obtain a user's web browsing history or historical location information.

While the Department of Justice's media subpoena and search warrant guidelines and the Privacy Protection Act, discussed above, partially protect journalists' records from search and

---

[34] *Id.* at § 50.10(a)(3).

[35] *See, e.g.*, P.L. 106-544, Section 7(a) Executive Branch Study on Administrative Subpoena Authority, Scope and Protections (2000) at I(A) (noting that "Agencies are limited in their exercise of administrative subpoena authority by: . . . agency promulgated guidelines limiting or directing subpoena issuance."), *available at* https://www.justice.gov/archive/olp/rpt_to_congress.htm#2a1; *id*. at App'x B (listing administrative subpoena authorities held by the Justice Department), *available at* https://www.justice.gov/archive/olp/rpt_to_congress.htm#appd_b.

[36] USAM 9-13.400(M)(1)(ix).

[37] *See* Office of the Attorney General, Updated policy regarding obtaining information from, or records of, members of the news media; and regarding questioning, arresting, or charging members of the news media (Jan. 14, 2015), *available at* http://www.justice.gov/file/317831/download.

seizure by the Justice Department, national security investigations are largely outside the scope of these statutory and regulatory protections, as the chart at Appendix A indicates. Although many national security authorities permit the government to collect and use the same type of communications metadata that they may otherwise obtain using a standard subpoena, the regulatory limits on subpoenas do not apply to these national security authorities. Certain national security processes allow the government to request and obtain journalists' records if the material is merely "relevant to an authorized investigation," even if the target is not suspected of a crime.

The wide array of legal mechanisms available to obtain information regarding communications can be overwhelming. Unfortunately, the overlapping and complex legal architecture for communications surveillance, coupled with widespread secrecy about government policies and capabilities, makes it difficult to understand how and under what circumstances the government can use its authority.

Understanding the risks posed by communications surveillance requires knowledge of two key concepts. First, surveillance authorities tend to distinguish between communications **content** and **metadata**. Second, statutes providing surveillance authority tend to distinguish between stored data, or information **at rest**, and real-time surveillance of information **in transit**. As a result, different requirements apply to the acquisition of real-time content or metadata than to stored content or historical metadata, and different statutes, described in detail below, authorize the acquisition of each type of information.

	At rest	In transit
Content	Search warrant (Fed. R. Crim. Proc. 41) SCA search warrant (18 U.S.C. § 2703(a)) SCA court order (18 U.S.C. § 2703(d)) Subpoena (grand jury, administrative, or trial) FISA search warrant	Wiretap Section 702 directive
Metadata	SCA court order (18 U.S.C. § 2703(d)) Subpoena (grand jury, administrative, or trial) National Security Letter Section 215 order	Pen Register/Trap and Trace (PR/TT) FISA PR/TT

A. Electronic Surveillance Authorities: Criminal Investigations

Journalists seeking to protect confidential sources need to be aware of the full range of legal authorities for surveillance in the context of criminal investigations as well as national security investigations. For example, government investigations of unauthorized leaks may use both criminal and national security investigative tools. Three of the most significant information-gathering authorities in the criminal context are the Stored Communications Act, the Pen Register Act, and the Wiretap Act.

Stored Communications Act, codified at 18 U.S.C. §§ 2701–2712

The Stored Communications Act authorizes the government to require providers of electronic communications services to disclose both the substantive **contents** of stored communications as well as the metadata **records** associated with those communications (*e.g.*, email dates, times, and header information, including "to" and "from" addresses).

The Stored Communications Act does not always require a warrant based on probable cause. Under Section 2703(a) of the Act, if a communication has been in storage for 180 days or less, the government must get a warrant in order to obtain the communications. Under Section 2703(b), if a communication has been in storage for more than 180 days, the government may obtain communications using an administrative subpoena or a court order based on "specific and articulable facts" showing that the communications are relevant to a criminal investigation if the government provides notice to the subscriber. Alternatively, it always remains the case that the government may obtain communications without providing notice if it obtains a traditional search warrant based on probable cause.[38]

Proposed legislation would require law enforcement to obtain a search warrant when it seeks the contents of communications, regardless of how long the communications have been in storage.[39] In addition, one federal appellate court has held that a warrant is required for the government to acquire communications content under the SCA,[40] and it is the policy of some internet companies to disclose communications content only pursuant to a search warrant.[41] One federal appellate court has also held that the SCA does not apply extraterritorially, which means that the government cannot get a warrant to seize email content stored exclusively on a foreign server.[42]

Under 18 U.S.C. § 2703(d), the government may obtain non-content subscriber records without notice using an administrative subpoena or a court order based on "specific and articulable facts" showing that the records are relevant to a criminal investigation.[43] A circuit split exists regarding the constitutionality of this provision as applied to the government's warrantless acquisition of historical cell site location information—information gleaned from cell towers that creates a record of an individual's location over time—and one party is petitioning to have the Supreme Court address the issue.[44]

---

[38] *See also Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*, *available at* https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ssmanual2009.pdf.
[39] Email Privacy Act, H.R. 699, 114th Cong. (2016).
[40] *Warshak*, 631 F.3d at 288 ("[T]o the extent that the SCA purports to permit the government to obtain such emails [stored with a commercial ISP] warrantlessly, the SCA is unconstitutional.").
[41] *See, e.g.*, Legal Process – Google Transparency Report, *available at* https://www.google.com/transparencyreport/userdatarequests/legalprocess/#whats_the_difference; *see also* Written Testimony of Richard Saldago, Director, Law Enforcement and Information Security at Google, Inc., Senate Judiciary Subcommittee on Privacy, Technology and the Law, Hearing on "The Surveillance Transparency Act of 2013" (Nov. 13, 2013), *available at* http://www.judiciary.senate.gov/imo/media/doc/11-13-13SalgadoTestimony.pdf.
[42] *In Matter of Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp*., 829 F.3d 197, 216 (2d Cir. 2016).
[43] The government may also obtain basic subscriber and session information using an administrative subpoena, trial subpoena, or grand jury subpoena. *See* 18 U.S.C. § 2703(c)(2).
[44] *See Graham v. United States*, Petition for Writ of Certiorari to the United States Court of Appeal for the Fourth Circuit, Case No. 16-6308 (2016) (set for conference on May 11, 2017), *available at* https://static1.squarespace.com/static/53e92769e4b07d7503ae637a/t/57eebe2cb3db2bd7ce270926/1475264044963/

In 2010, the United States Attorney for the District of Columbia sought and obtained a search warrant under 18 U.S.C. § 2703(a) for the personal email account of James Rosen, a Fox News reporter, in connection with an investigation of unauthorized disclosure of classified information that Rosen had published in a 2009 article. In that case, the government obtained a warrant for the disclosure of "any and all communications" between Rosen's email address and three specified email addresses, in addition to "any and all communications" to or from Rosen's email address on the two days following the publication of Rosen's article. In the probable cause affidavit in support of its warrant application, the government argued that Rosen had conspired with his source to violate the Espionage Act and that the search was therefore permissible under the "suspect exception" to the Privacy Protection Act.[45] In addition, the Justice Department took the position that email search warrants obtained under the Stored Communications Act did not require notice to customers and subscribers whose accounts were searched.[46] According to press accounts, Rosen did not learn of the search until nearly three years later.[47]

At the time of the Rosen search, the Attorney General's policy on obtaining records of members of the news media did not specifically apply to search warrants, although news reports indicate that then-Attorney General Eric Holder nonetheless personally approved the warrant.[48] Today, the Department of Justice media subpoena guidelines apply to search warrants as well as to court orders issued under Section 2703(a)–(d) of the Stored Communications Act, requiring the government to pursue notice and negotiation with a member of the news media and to meet substantive tests before seeking a journalist's communications or records using these tools. However, if a search warrant, subpoena, or court order is approved in a matter where the reporter is a subject or target, as opposed to a witness, the Department is *not* required to pursue notice and negotiation with the journalist. To protect journalists from being targeted in investigations directed at their sources, however, the revised guidelines also indicate that a search warrant for a journalist's records should not be approved if its "sole purpose" is in support of an investigation of a different person.[49] This seemed to be the case in the Rosen matter, and Holder has stated that he regretted identifying Rosen as a "co-conspirator" in the probable case affidavit.[50] Notwithstanding these protections, as indicated earlier, the guidelines explicitly state that they do not create any enforceable rights.[51]

Last year, Microsoft initiated a legal challenge to Section 2705 of the SCA, which permits the government to apply for a gag order when they are executing warrants pursuant to

---

2016-09-30+Graham+cert+petition+CORRECTED.pdf. *See also* Am. Civ. Lib. Union, Cell Phone Location Tracking Laws By State, *available at* https://www.aclu.org/map/cell-phone-location-tracking-laws-state.

[45] *See* Dep't of Justice Report on Review of News Media Policies, *supra*, at 3.

[46] *See* Ryan Lizza, *How Prosecutors Fought to Keep Rosen's Warrant Secret*, The New Yorker (May 24, 2013) *available at* http://www.newyorker.com/news/news-desk/how-prosecutors-fought-to-keep-rosens-warrant-secret.

[47] *Id*.

[48] *Id.*

[49] 28 C.F.R. § 50.10(d)(5).

[50] *See Holder says 'subpoena' to Fox News reporter is his one regret*, Fox News (Oct. 30, 2014), *available at* http://www.foxnews.com/politics/2014/10/29/holder-says-subpoena-to-fox-news-reporter-is-his-one-regret.html; *see also* Charlie Savage, *Holder Hints Reporters May Be Spared Jail in Leak*, N.Y. Times (May 27, 2014) (Holder stating, "As long as I'm attorney general, no reporter who is doing his job is going to go to jail. As long as I'm attorney general, someone who is doing their job is not going to get prosecuted."), *available at* http://www.nytimes.com/2014/05/28/us/holder-hints-reporter-may-be-spared-jail-in-leak.html.

[51] *Id.* at (j).

Section 2703.[52] The Section 2705 gag order prevents companies like Microsoft from telling their customers that their records were searched. Microsoft argued in federal district court in Seattle that these gag orders violated both the First and Fourth Amendments. In February of this year, the judge in that case allowed the case denied the government's motion to dismiss Microsoft's First Amendment claims, but granted the motion as to the Fourth Amendment claims, concluding that Microsoft lacked standing to assert its customers' Fourth Amendment rights. The case is ongoing.

Pen Registers and Trap and Trace Devices, codified at 18 U.S.C. §§ 3121–3127

The so-called "Pen/Trap" statute regulates the collection of non-content information related to electronic communications in real time. Pen registers and trap and trace ("PR/TT") orders authorize the government to obtain communications metadata, such as the phone numbers associated with incoming and outgoing calls, or the email addresses of a sender and recipient.[53] The Pen Register Act requires a federal court to "enter an ex parte order authorizing the installation and use of a pen register or trap and trace device" on a facility or other service belonging to a wire or electronic communication service provider.[54] In order to obtain the order, the government must certify that "the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation."[55] Pen register/trap and trace orders are sealed and accompanied by a gag order directing the communication service provider not to disclose the existence of the order. The Attorney General's policy on obtaining records of members of the news media applies to PR/TT orders.

Wiretap Act, codified at 18 U.S.C. §§ 2510–2522

The Wiretap Act authorizes the government to make an application to a federal judge for an order—often referred to as a "Title III" order given the placement of the Wiretap Act in the 1968 omnibus crime legislation—authorizing the real-time interception of wire, oral, or electronic communications. The Act requires the government to demonstrate probable cause to believe that an individual is committing a criminal offense, and that the places where the interception is to occur—*e.g.*, the phone line or online account—"are being used, or are about to be used, in connection with the commission" of that offense.[56] The Department of Justice media subpoena guidelines do not apply to applications under the Wiretap Act, but the Act does require advance departmental review and approval before applications for certain types of electronic surveillance may be submitted to a court. Specifically, 18 U.S.C. § 2516(1) requires that the Attorney General review and approve such applications, but the Attorney General may delegate this authority to certain enumerated high-level Justice Department officials, such as the Deputy Assistant Attorneys General for the Criminal Division. Moreover, the government must minimize the interception of communications not otherwise subject to interception under the order, and minimize the duration of the interception by terminating the surveillance once the

[52] *Microsoft v. Dept. of Justice*, Case No. 2:16-cv-00538-JLR (W.D. Wash. Jun. 17, 2016).
[53] 18 U.S.C. § 3127.
[54] 18 U.S.C. § 3123(a).
[55] *Id*.
[56] 18 U.S.C. § 2518.

conversation sought is seized.[57] Interception periods must be no longer than thirty days, but the court may extend this period under certain circumstances.[58]

B. National Security Letters

NSLs are warrantless requests issued by high-ranking FBI officials and directed at third parties for *non-content* records. The FBI may issue an NSL compelling disclosure of subscriber records— *i.e.*, metadata—if it certifies that the records sought are relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities. Unless the recipient challenges the NSL, the request is not subject to judicial review.

Four statutes authorize the use of NSLs to obtain subscriber information from third parties, such as telephone companies, internet service providers, financial service providers, and credit institutions.[59] By far the most commonly used NSL authority is a provision in the Electronic Communications Privacy Act (ECPA), which enables the FBI to request the "local and long distance toll billing records" of any person from a "wire or electronic communication service provider."[60]

Over ninety percent of NSLs are issued with gag orders prohibiting the third party from informing the subscriber that the government requested the subscriber's information.[61] The FBI may accompany an NSL with a gag order if "otherwise there *may* result a danger to the national security of the United States, interference with a criminal, counterterrorism, or counterintelligence investigation, interference with diplomatic relations, or danger to the life or physical safety of *any* person.…" The gag orders typically have no expiration date. In 2014, the Reporters Committee filed an amicus brief in a constitutional challenge to ECPA's NSL provision arguing that the gag orders are unconstitutional prior restraints, and that the atmosphere of secrecy surrounding NSLs obscures surveillance efforts by the government and chills reporter-source communications.[62] That case was remanded to the lower court in light of 2015 reforms to the NSL statute pursuant to the 2015 USA FREEDOM Act. These reforms required the Attorney General to adopt new procedures for NSL gag orders that require "review at appropriate intervals" and termination of nondisclosure obligations if they are no longer necessary.[63] Under these NSL procedures, when an investigation ends, the gag order must be lifted unless the FBI makes a determination that one of a number of statutory standards for

---

[57] *See* 18 U.S.C. § 2518(5); *see also Nixon v. Administrator of General Services*, 433 U.S. 425, 463 (1977); *Berger v. New York*, 388 U.S. 41, 55 (1967).
[58] *See* 18 U.S.C. § 2518(5).
[59] These statutes are the Electronic Communications Privacy Act (18 U.S.C. § 2709), the National Security Act (50 U.S.C. § 3162), the Right to Financial Privacy Act (12 U.S.C. § 3414), and the Fair Credit Reporting Act (15 U.S.C. §§ 1681u, v.).
[60] 18 U.S.C. § 2709.
[61] Office of the Inspector General, *A Review of the Federal Bureau of Investigation's Use of National Security Letters: Assessment of Corrective Actions and Examination of NSL Usage in 2006* 124 (Mar. 2008) ("Of the 375 NSLs we examined in our random sample, 365, or 97 percent imposed the non-disclosure and confidentiality obligation established in the Patriot Reauthorization Act. Based on that result, we projected that of the 15,187 NSLs the FBI issued from March 10, 2006, through December 31, 2006, 14,782 NSLs imposed the non-disclosure and confidentiality obligations."), *available at* https://oig.justice.gov/reports/2014/s1410a.pdf.
[62] Amicus Br. in Support of Petitioner-Appellant, *Under Seal v. Holder et al.*, Nos. 13-15957, 13-16731 (9th Cir. filed Apr. 9, 2014), *available at* https://rcfp.org/sites/default/files/2014-06-10-in-re-national-security-letter.pdf.
[63] Termination Procedures for National Security Letter Nondisclosure Requirement, *available at* https://www.fbi.gov/file-repository/nsl-ndp-procedures.pdf/view.

nondisclosure is satisfied.[64] The FBI is also required to review the gag order three years after the investigation begins to determine whether one of the statutory exceptions applies.[65]

The FBI has used NSLs to compel electronic communications service providers to disclose data including web browsing history and online purchases.[66] Because of the pervasive secrecy surrounding NSL procedures, it remains unconfirmed whether the FBI has obtained communications records of journalists using NSLs. However, several incidents of abuse implicating reporters' rights have come to light in recent years regarding similar instruments.

These incidents involved processes that, like NSLs, were not subject to judicial review. In 2007, during the first review of NSL usage by the Office of the Inspector General for the Department of Justice ("OIG"), the OIG found that the FBI had frequently sought telephone toll billing records or subscriber information by using an "exigent letter," an informal request, rather than NSLs or grand jury subpoenas.[67] The OIG identified three leak investigations in which journalists' records had been requested using methods that did not comply with the Department of Justice guidelines.[68] Under the version of the guidelines then in place, the Attorney General was required to approve the issuance of subpoenas for reporters' records. The OIG found that by using an "exigent letter," the FBI was functionally circumventing the guidelines' requirement to seek Attorney General approval.

In one instance, the FBI obtained phone records for *Washington Post* reporters Ellen Nakashima and Alan Sipress, *Washington Post* researcher Natasha Tampubolon, and *New York Times* reporters Raymond Bonner and Jane Perlez using an exigent letter that claimed a grand jury subpoena was forthcoming; none was. In response to the exigent letter, the phone provider produced 22 months of records for Ellen Nakashima, and 22 months of records for the *Washington Post* bureau in Jakarta.[69] The OIG report called this production of materials "a complete breakdown in the required Department [of Justice] procedures for approving the issuance of grand jury subpoenas for reporters' toll billing records."[70] While the OIG did not address the availability of NSL practice in this instance or the others involving journalists, its concerns about the abuse of exigent letters could not have been more clear or emphatic.

The Department of Justice and the FBI have taken the position that the guidelines do not apply to NSLs.[71]

---

[64] *Id*. at 2.
[65] *Id*.
[66] Dustin Volz, *U.S. government reveals breadth of requests for Internet records*, Reuters (Dec. 1, 2015), *available at* www.reuters.com/article/us-usa-cybersecurity-nsl-idUSKBN0TJ2PJ20151201.
[67] *See* Office of the Inspector General, *A Review of the Federal Bureau of Investigation's Use of National Security Letters* 86–97 (Mar. 2007), *available at* https://oig.justice.gov/special/s0703b/final.pdf.
[68] *See* Office of the Inspector General, *A Review of the Federal Bureau of Investigation's Use of Exigent Letters and Other Informal Requests for Telephone Records* 89–121 (Jan. 2010), *available at* https://oig.justice.gov/special/s1001r.pdf.
[69] *Id*. at 95–97.
[70] *Id*. at 103.
[71] *See* DIOG App. § G.12 ("The [28 C.F.R. § 50.10] regulation concerns *only* grand jury subpoenas, not National Security Letters (NSLs) or administrative subpoenas."); Amicus Brief at 7–8, *Freedom of the Press Foundation v. Dep't of Justice*, No. 15-cv-3503-HSG (N.D. Cal. Jun. 10, 2016), ECF No. 36 (*available at* https://rcfp.org/browse-media-law-resources/briefs-comments/freedom-press-foundation-v-dept-justice).

DOJ Media Guidelines (28 C.F.R. § 50.10)	FBI NSL Policy (DIOG App'x G)[72]
Information sought must be "essential to a successful investigation, prosecution, or litigation." 28 C.F.R. § 50.10(a)(3).	Information sought must be "relevant" to a national security investigation. DIOG § 18.6.6.3.3.
The requester must make "reasonable alternative attempts . . . to obtain the information from alternative sources." 28 C.F.R. § 50.10(a)(3).	No requirement to use alternative methods to obtain information.
The requester must notify and negotiate with the member of the news media before the search, unless the Attorney General determines there is a clear and substantial threat to the integrity of the investigation, grave harm to national security, or imminent risk of death or bodily harm. 28 C.F.R. § 50.10(a)(3), (4).	There is no requirement to notify news media, and the NSL is usually accompanied by a gag order preventing the third party from notifying the subscriber or news media.[73]
The requester must obtain a request for authorization personally endorsed by the United States Attorney or Assistant Attorney General (28 C.F.R. § 50.10(c)(2)), and authorization by the Attorney General (28 C.F.R. § 50.10(c)(1)).	To issue an NSL for news media records, the requester must obtain authorization by the FBI General Counsel and the Executive Assistant Director of the FBI's National Security Branch. DIOG App'x § G.12 Approval requirements.
In investigations of unauthorized disclosures of national defense or classified information, the requester must obtain an additional certification from the Director of National Intelligence before requesting Attorney General authorization. 28 C.F.R. § 50.10(c)(4)(vi).	To issue an NSL seeking news media's confidential sources, the requester must also consult with the Assistant Attorney General for the Justice Department's National Security Division. DIOG App'x § G.12 Approval requirements.

C. Electronic Surveillance Authorities: Foreign Intelligence

In foreign intelligence and national security investigations, the government has additional statutory authorities that enable it to conduct electronic communications surveillance. While the government may use ordinary wiretaps and pen registers in investigations touching on national security, it also possesses expanded authority under provisions of the Foreign Intelligence Surveillance Act (FISA) as well as the USA PATRIOT Act. The scope and secrecy of FISA-related surveillance has raised particular concerns that digital newsrooms could be searched using a FISA court order.

Foreign Intelligence Surveillance Act—Overview

The Foreign Intelligence Surveillance Act authorizes electronic and physical surveillance of foreign powers and agents of foreign powers for the purpose of collecting "foreign intelligence information." FISA was originally enacted in 1978 to regulate the collection of foreign intelligence information within the United States. Until 2001, FISA permitted electronic and physical surveillance of "foreign powers" and "agents of foreign powers" if foreign

[72] *Available at* https://www.documentcloud.org/documents/2934087-DIOG-Appendix-Media-NSLs.html.
[73] Office of the Inspector General, *A Review of the Federal Bureau of Investigation's Use of National Security Letters: Assessment of Corrective Actions and Examination of NSL Usage in 2006, supra,* 124.

intelligence collection was the "primary purpose" of the activity. In 2001, the USA PATRIOT Act amended FISA to allow searches if foreign intelligence collection was a "significant purpose."

"Foreign intelligence information" is a broad term, and includes information that pertains to a variety of dangers related to "foreign powers" as well as "information with respect to a foreign power or foreign territory that relates to, and if concerning a United States person is necessary to--(A) the national defense or the security of the United States; or (B) the conduct of the foreign affairs of the United States."[74] In addition, the PATRIOT Act relaxed the standards for acquiring metadata through PR/TT orders and for orders compelling production of business records or "tangible things" relevant to an investigation to obtain foreign intelligence information. This authority, known as Section 215, was the statutory authority for the bulk telephony metadata collection program disclosed by former NSA contractor Edward Snowden in 2013. As discussed below, Section 215 expired on June 1, 2015, and the USA FREEDOM Act ended the government's bulk collection of telephone records in November 2015.[75]

Beginning in 2007, Congress enacted a series of amendments to FISA intended to broaden its scope to authorize electronic surveillance of foreigners abroad.[76] In 2007 and 2008, Congress enacted further amendments to FISA that created statutory authority to conduct programmatic surveillance on non-United States persons outside the United States. This provision, commonly known as Section 702, is the statutory authority for some of the other activities disclosed by Snowden, including bulk collection of the contents of electronic communications outside the United States.[77]

Traditional FISA: Electronic and Physical Searches, codified at 50 U.S.C. §§ 1801–1829

"Traditional" FISA orders authorize electronic and physical surveillance *within* the United States of targets who are foreign powers or agents of foreign powers.[78] Electronic surveillance includes the acquisition of communications content. (Acquisition of communications metadata, under the FISA definition, is not "electronic surveillance"; rather, domestic metadata collection is governed by Section 215, discussed below.)

Traditional FISA orders require the government to identify a specific target for surveillance and to demonstrate probable cause to believe that the target of surveillance is a foreign power or an agent of a foreign power.[79] In addition, FISA's electronic surveillance provision requires the Attorney General to adopt "minimization procedures" that are designed "to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly

[74] 50 U.S.C. § 1801.
[75] USA FREEDOM Act of 2015, Pub. L. 114-23, Sec. 107 (2015).
[76] *See* Protect America Act of 2007, Pub. L. 110-55 (2007); FISA Amendments Act of 2008, Pub. L. 110-261 (2008).
[77] *See NSA Slides Explain the PRISM Data-Collection Program*, Wash. Post (Jun. 6, 2013), *available at* http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/.
[78] 50 U.S.C. § 1801 (defining "foreign power," "agent of a foreign power," and "electronic surveillance").
[79] 50 U.S.C. § 1805 (requiring probable cause for electronic surveillance); 50 U.S.C. § 1824 (requiring probable cause for physical surveillance).

available information concerning unconsenting United States persons."[80] Each application is reviewed by a judge on the Foreign Intelligence Surveillance Court (FISC).

FISA PR/TT Orders, codified at 50 U.S.C. §§ 1841–1846

The government may obtain a FISA PR/TT order in an "investigation to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities."[81] FISA PR/TTs may be used to monitor telephone calls and electronic communications.

FISA PR/TT requests do not require the government to demonstrate probable cause that the target is a foreign power or an agent of a foreign power. Rather, the government must certify that the information at issue is "relevant" to an authorized investigation.[82] However, under the USA FREEDOM Act of 2015, the government is required to use a "specific selection term" (SST) to identify a person, account, device, or other personal identifier as the basis for use of the PR/TT device and to ensure that the PR/TT provision is not used for impermissible bulk collection.[83]

Section 702 of the FISA Amendments Act, codified at 50 U.S.C. § 1881a

Like FISA's traditional electronic surveillance provision, Section 702 of the FISA Amendments Act of 2008 authorizes the collection of communications content, but the provision's procedures and safeguards differ dramatically from traditional FISA. Section 702 is intended to permit electronic foreign intelligence surveillance of non-U.S. persons located abroad, regardless of whether there is probable cause to believe that those persons are foreign powers or agents of foreign powers. In contrast, traditional FISA electronic surveillance occurs on U.S. soil.

Accordingly, Section 702 grants authority for the government to obtain directives compelling electronic communication service providers to enable surveillance of communications of non-United States persons located abroad, without mandating that the government identify a specific target. Section 702 requires the government to annually provide to the FISC a written, sworn certification attesting that there are "targeting procedures" in place that are "reasonably designed" to ensure that surveillance is "limited to targeting persons reasonably believed to be located outside the United States" and to avoid "intentional acquisition" of communications when the sender and all recipients are known to be located in the United States.[84]

Because Section 702 authorizes "electronic surveillance," it also requires the Attorney General and the Director of National Intelligence to adopt minimization procedures. The minimization and targeting procedures required by Section 702 are subject to judicial review and approval by the FISC. It is unclear, however, whether the minimization procedures comport with the Privacy Protection Act's statutory ban on newsroom searches.[85] Section 702 is the legal

---

[80] *Id*. at (a)(3), (c)(2)(A); 50 U.S.C. § 1801(h) (defining minimization procedures).
[81] 50 U.S.C. § 1842(a)(1).
[82] *Id*. at (c)(2).
[83] USA FREEDOM Act of 2015, Pub. L. 114-23, Sec. 201.
[84] 50 U.S.C. § 1881a(d).
[85] *See supra* Part II.B at 6.

authority supporting "upstream" collection as well as the PRISM program, both of which facilitate collection of the contents of communications in bulk and without suspicion.[86]

Organizations have repeatedly challenged the constitutional and statutory basis of bulk surveillance. In 2008, the Electronic Frontier Foundation filed a lawsuit, *Jewel v. National Security Agency*, challenging "upstream" surveillance (as well as other bulk collection activities) on behalf of AT&T customers whose communications and telephone records were collected by the NSA.[87] Last year, the district court rejected the plaintiffs' Fourth Amendment arguments, but has not issued a ruling on their First Amendment claims, and the case is currently in discovery.[88]

In addition, Wikimedia, PEN American Center, and The Nation Magazine, among other organizations, filed a lawsuit challenging "upstream" surveillance of online communications, raising both First Amendment and Fourth Amendment arguments.[89] The *Wikimedia* plaintiffs claim that upstream surveillance impedes their journalism, advocacy, and publishing activities. The district court ruled against Wikimedia in 2015, and an appeal is pending before the Fourth Circuit.[90] (The Reporters Committee filed an amicus brief in that case on behalf of itself and 17 news media organizations, arguing that upstream surveillance chills newsgathering and violates the First and Fourth Amendments.[91])

Section 215 of the PATRIOT Act, codified at 50 U.S.C. § 1861

Section 215 provided authority for the government to obtain "tangible things" relevant to an investigation to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities.[92] Orders for the production of tangible things, or "business records" orders, authorized the government to request the business records of third parties, such as customer transactional records. Section 215 was the authority under which the government maintained the bulk telephony metadata program, which had collected all domestic calling records without suspicion on an ongoing basis.[93]

Section 215 expired on June 1, 2015, and the USA FREEDOM Act ended the government's bulk collection of telephone records at the end of November 2015.[94] Under the revised statute, the government must use a "specific selection term" (SST) to identify a person, account, device, or other personal identifier as the basis for production of call detail records. In

---

[86] *See* James Ball, *NSA's Prism surveillance program: how it works and what it can do*, The Guardian (Jun. 8, 2013), *available at* www.theguardian.com/world/2013/jun/08/nsa-prism-server-collection-facebook-google.
[87] *Jewel v. NSA*, No. C 08-04373 (N.D. Cal. 2018).
[88] *Id.*; *see also* Jamie Williams, *Jewel v. NSA Moves Forward—Time for NSA to Answer Basic Questions About Mass Surveillance*, Electronic Frontier Foundation (Jun. 21, 2016), *available at* https://www.eff.org/deeplinks/2016/06/jewel-v-nsa-moves-forward-time-nsa-answer-basic-questions-about-mass-surveillance.
[89] *Wikimedia Foundation v. NSA*, No. 15CV00662 (D. Md. 2015).
[90] *See* Order Granting Defendants' Motion to Dismiss, *Wikimedia Foundation v. NSA*, No. 15CV00662, Dkt. 95 (filed Oct. 23, 2015); *Wikimedia Foundation v. NSA*, No. 15-2560 (4th Cir. 2016).
[91] Amicus Br. in Support of Plaintiffs-Appellants, *Wikimedia v. NSA*, No. 15-2560 (4th Cir. filed Feb. 24, 2016), *available at* https://www.rcfp.org/sites/default/files/2016-02-24-wikimedia-v-nsa.pdf.
[92] 50 U.S.C. § 1861(a)(1).
[93] *See, e.g.,* Glenn Greenwald, *NSA collecting phone records of millions of Verizon customers daily*, The Guardian (Jun. 6, 2013), *available at* https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order.
[94] USA FREEDOM Act of 2015, Pub. L. 114-23, Sec. 107.

the current framework, rather than collecting the call detail records itself, the government requests records pertaining to a specific selector from a telephone carrier.

It remains unclear how the end of bulk collection of telephony metadata under Section 215 will impact the several ongoing challenges to the constitutionality of that provision. In early 2015, shortly before the passage of USA FREEDOM, the Second Circuit ruled in ACLU v. Clapper that the bulk collection of telephony metadata was not authorized by Section 215.[95] In November 2015, the District Court for the District of Columbia granted a preliminary injunction barring the government from collecting plaintiffs' telephony metadata under the bulk collection program, and the injunction was stayed pending appeal.[96] In January 2016, the government filed a motion to vacate the preliminary injunction as moot in light of the change in law and government policy, stating that "bulk collection of telephony metadata under Section 215 has ceased, analytic queries of such previously-collected metadata has likewise ended, and the government has transitioned to a new intelligence program based on targeted rather than bulk collection of telephony metadata."[97] Similarly, a Ninth Circuit challenge to the bulk telephony metadata program on Fourth Amendment grounds, Smith v. Obama, was partially dismissed as moot in early 2016.[98] Executive Order 12333

In addition to the other authorities discussed above, the Intelligence Community also conducts communications surveillance activities abroad under Executive Order 12333 ("EO 12333"),[99] a 1981 presidential order setting out general contours and guidelines for intelligence-gathering. EO 12333 places constraints on the use of these surveillance programs to target communications of United States persons.[100] However, some have argued that collection activities are so broad and sweeping that any constraints are relatively trivial.[101] EO 12333 appears to permit the collection of actual communications content — not just metadata — of U.S. citizens so long as the communications are collected "incidentally" to authorized activities. Moreover, many of the minimization procedures[102] that constrain government use of information collected pursuant to EO 12333 remain classified, and the limited information that is publicly available only gives vague guidance as to protections in place for First Amendment activity. Likewise, many of the programs conducted under EO 12333 are secret as well.

---

[95] *ACLU v. Clapper*, 785 F.3d 787, 818–19, 826 (2d Cir. 2015).
[96] *Klayman v. Obama*, 142 F. Supp. 3d 172, 198 (D.D.C. 2015).
[97] *See* Motion to Vacate Preliminary Injunction and Dismiss Appeal on Grounds of Mootness, *Klayman v. Obama*, No. 15-5307, 2 (D.C. Cir. filed Jan. 4, 2016); *see also* Order, *Klayman v. Obama*, No. 15-5307 (D.C. Cir. filed Apr. 4, 2016) (dismissing appeal as moot).
[98] *Smith v. Obama*, 816 F.3d 1239, 1241 (9th Cir. 2016), *available at* https://www.eff.org/cases/smith-v-obama; *see also* Amicus Br. in Support of Plaintiff-Appellant, *Smith v. Obama*, No. 14-35555 (9th Cir. filed Sept. 9, 2014), *available at* https://www.rcfp.org/sites/default/files/2014-09-09-smith-v-obama.pdf (arguing that mass call tracking impedes confidentiality, chills reporters and sources, and is overbroad).
[99] Exec. Order No. 12333, United States Intelligence Activities, 46 Fed. Reg. 59941 (Dec. 4, 1981) (as amended at 73 Fed. Reg. 45325 (2008)), *available at* https://www.archives.gov/federal-register/codification/executive-order/12333.html.
[100] *Id*. at 59950.
[101] *See, e.g.,* John Napier Tye, *Meet Executive Order 12333: The Reagan rule that lets the NSA spy on Americans*, Wash. Post (Jul. 18, 2014), *available at* https://www.washingtonpost.com/opinions/meet-executive-order-12333-the-reagan-rule-that-lets-the-nsa-spy-on-americans/2014/07/18/93d2ac22-0b93-11e4-b8e5-d0de80767fc2_story.html.
[102] Attorney General Approved U.S. Person Procedures Under E.O. 12333, Civil Liberties and Privacy Office of the Office of the Director of National Intelligence (Feb. 10, 2015), *available at* https://www.pclob.gov/library/EO12333-AG-Guidelines-February-10-2015.pdf.

IV. CONCLUSION

Understanding the variety of legal authorities and mechanisms that the government relies upon in conducting surveillance is crucial to assessing the relative risks to journalists and sources who use these electronic communications technologies. The chart in Appendix A summarizes key aspects of legal and policy protections in the context of these authorities. Journalists concerned about securing their communications, or interested in adopting technical measures to enhance privacy or confidentiality, may be interested in exploring how their newsgathering practices might implicate information at rest and in transit, as well as how they might protect their content and metadata. Appendix B offers a number of resources for journalists and reporters interested in experimenting with and implementing secure communications protocols themselves.

APPENDIX A

Type of process	Standard	Type of information sought	Issued by	Covered by Guidelines	Covered by PPA
Subpoena (administrative, grand jury, or trial)	Relevance to a lawful purpose	Communications content (opened, sent, or older than 180 days) (only with notice); basic subscriber and session information	Agency (administrative subpoena) or with court oversight (grand jury or trial subpoena)	Yes	Yes (if content); no (if subscriber/session information)
Search Warrant	Probable cause	Communications content, metadata, and/or basic subscriber and session information	Court	Yes	Yes
2703(d) Order	"Specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation"	Communications content (opened, sent, or older than 180 days) (only with notice); basic subscriber and session information; communications metadata	Court	Yes	Yes (if content); no (if metadata or subscriber/session information)
PR/TT	Government certification "that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation"	Dialing, routing, addressing, or signaling information	Court	Yes	No
Wiretap (Title III)	Probable cause that an individual is committing or has committed an enumerated offense; probable cause "that particular communications concerning that offense will be obtained through such interception; normal investigative procedures have been	Communications content	Court	No	Yes

	tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous; the facilities from which, or the place where, the wire, oral, or electronic communications are to be intercepted are being used, or are about to be used, in connection with the commission of such offense"				
FISA warrant	Probable cause to believe that the target "is a foreign power or an agent of a foreign power, except that no United States person may be considered an agent of a foreign power solely upon the basis of activities protected by the first amendment to the Constitution of the United States," and the place or thing to be searched "is being used, or is about to be used, by a foreign power or an agent of a foreign power"	Communications content and metadata	FISA Court	No	Yes
FISA PR/TT	Relevance to "any investigation to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon" the basis of First Amendment activities	Dialing, routing, addressing, or signaling information	FISA Court	No	No
FISA Section 215	Relevance to "an investigation to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not	Tangible things (including books, records, papers, documents, and other items)	FISA Court	No	No

	conducted solely upon" the basis of First Amendment activities				
FISA Section 702	Targeting persons reasonably believed to be located outside the United States to acquire foreign intelligence information while employing approved minimization procedures	Communications content and metadata	FISA Court	No	No
NSL	Relevance to an "open, predicated national security investigation," provided that "such an investigation of a United States person is not conducted solely upon the basis of" First Amendment activities	Communications metadata; subscriber information	FBI	No	No

APPENDIX B

Digital security resources

1. Committee to Protect Journalists, "Journalist Security Guide" https://cpj.org/security/guide.pdf

2. Digital Defenders Project, "The Digital First Aid Kit" https://www.digitaldefenders.org/digitalfirstaid/

3. Electronic Frontier Foundation, "Surveillance Self-Defense" https://ssd.eff.org/

4. Free Software Campaign, "Email Self-Defense Guide" https://emailselfdefense.fsf.org/en/

5. Reporters Without Borders, "Online Survival Kit" https://rsf.org/en/online-survival-kit

6. Tactical Technology Collective, "The Holistic Security Manual" https://holistic-security.tacticaltech.org/

7. Tactical Technology Collective and Front Line Defenders, "Security In-A-Box" https://tacticaltech.org/projects/security-box

Legal Reports

1. Privacy and Civil Liberties Oversight Board, *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act* (July 2, 2014), *available at* https://pclob.gov/library/702-Report-2.pdf.

2. Privacy and Civil Liberties Oversight Board, *Report on the Telephone Records Program Conducted under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court* (Jan. 23, 2014), *available at* https://pclob.gov/library/215-Report_on_the_Telephone_Records_Program.pdf.