BRENNAN
CENTER
FOR JUSTICE
TWENTY
YEARS

OVERSEAS SURVEILLANCE IN AN INTERCONNECTED WORLD

Amos Toh, Faiza Patel, and Elizabeth Goitein

Brennan Center for Justice *at New York University School of Law*

ABOUT THE BRENNAN CENTER FOR JUSTICE

The Brennan Center for Justice at NYU School of Law is a nonpartisan law and policy institute that seeks to improve our systems of democracy and justice. We work to hold our political institutions and laws accountable to the twin American ideals of democracy and equal justice for all. The Center's work ranges from voting rights to campaign finance reform, from ending mass incarceration to preserving constitutional protection in the fight against terrorism. Part think tank, part advocacy group, part cutting-edge communications hub, we start with rigorous research. We craft innovative policies. And we fight for them — in Congress and the states, the courts, and in the court of public opinion.

ABOUT THE BRENNAN CENTER'S LIBERTY AND NATIONAL SECURITY PROGRAM

The Brennan Center's Liberty and National Security Program works to advance effective national security policies that respect constitutional values and the rule of law, using innovative policy recommendations, litigation, and public advocacy. The program focuses on reining in excessive government secrecy; ensuring that counterterrorism authorities are narrowly targeted to the terrorist threat; and securing adequate oversight and accountability mechanisms.

ABOUT THE BRENNAN CENTER'S PUBLICATIONS

Red cover | Research reports offer in-depth empirical findings.
Blue cover | Policy proposals offer innovative, concrete reform solutions.
White cover | White papers offer a compelling analysis of a pressing legal or policy issue.

ABOUT THE AUTHORS

Amos Toh serves as Legal Advisor to the UN Special Rapporteur on the right to freedom of opinion and expression, and advises the Rapporteur on issues relating to freedom of expression in the digital age. From 2012 to 2015, Mr. Toh served as Counsel and Katz Fellow at the Brennan Center for Justice, where he worked on surveillance and efforts to combat religious discrimination in counterterrorism activities. Mr. Toh received an LL.M. from the NYU School of Law and a Bachelor of Laws from the National University of Singapore School of Law. This report does not purport to represent the views of the United Nations Special Rapporteur.

Faiza Patel serves as co-director of the Brennan Center for Justice's Liberty and National Security Program. She has testified before Congress opposing the dragnet surveillance of Muslims, organized advocacy efforts against state laws designed to incite fear of Islam, and developed legislation creating an independent Inspector General for the NYPD. Before joining the Brennan Center, Ms. Patel worked as a senior policy officer at the Organization for the Prohibition of Chemical Weapons in The Hague, and clerked for Judge Sidhwa at the International Criminal Tribunal for the former Yugoslavia. Born and raised in Pakistan, Ms. Patel is a graduate of Harvard College and the NYU School of Law.

Elizabeth (Liza) Goitein co-directs the Brennan Center for Justice's Liberty and National Security Program. Before coming to the Brennan Center, Ms. Goitein served as counsel to Sen. Russell Feingold, Chairman of the Constitution Subcommittee of the Senate Judiciary Committee. As counsel to Sen. Feingold, Ms. Goitein handled a variety of liberty and national security matters, with a particular focus on government secrecy and privacy rights. Previously, Ms. Goitein was a trial attorney in the Federal Programs Branch of the Civil Division of the Department of Justice. Ms. Goitein graduated from the Yale Law School and clerked for the Honorable Michael Daly Hawkins on the U.S. Court of Appeals for the Ninth Circuit.

ACKNOWLEDGEMENTS

The Brennan Center gratefully acknowledges The Atlantic Philanthropies, The Bauman Foundation, The Herb Block Foundation, CS Fund, Democracy Alliance Partners, Ford Foundation, and Open Society Foundations for their generous support of the Liberty & National Security Program.

The authors would like to thank the Brennan Center's Michael Waldman and John Kowal for their invaluable input and support; Brynne O'Neal and Meghan Koushik for their diligent research assistance; and Jeanine Plant-Chirlin, Jim Lyons, Seth Hoy, Naren Daniel, Theresa Jefferson and Desire Vincent for their editing and communications guidance. In addition, the authors benefited greatly from conversations and correspondence with Alex Abdo, Jennifer Daskal, Laura Donohue, Neema Singh Guliani, Deborah Pearlstein, Margo Schlanger, Patrick Toomey, John Napier Tye, Cynthia Wong, and Harlan Yu.

TABLE OF CONTENTS

OVERSEAS SURVEILLANCE IN AN INTERCONNECTED WORLD

"*There are very few things we cannot accomplish within the existing rules, using the authorities we have and those authorities we can receive.*" — NSA training slide, slide no. 83.[1]

EXECUTIVE SUMMARY

Since Edward Snowden's 2013 revelations about National Security Agency ("NSA") spying, there has been an ongoing public debate about the size and scope of the government's domestic surveillance operations. Snowden's disclosure about the NSA's gathering of millions of Americans' telephone records has already spurred Congress to set new limits on domestic bulk data collection. And next year, a provision of the Foreign Intelligence Surveillance Act authorizing the warrantless domestic collection of communications between Americans and foreigners will expire unless reauthorized. A spirited discussion about whether and how that law should be extended has already begun.

In contrast, there has been relatively little public or congressional debate within the United States about the NSA's overseas surveillance operations, which are governed primarily by Executive Order (EO) 12333—a presidential directive issued by Ronald Reagan in 1981 and revised by subsequent administrations. These activities, which involve the collection of communications content and metadata alike, constitute the majority of the NSA's surveillance operations, yet they have largely escaped public scrutiny.

There are several reasons why EO 12333 and the programs that operate under its aegis have gone largely unnoticed. One is the misconception that overseas surveillance presents little privacy risk to Americans. Another is the scant information in the public domain about how EO 12333 actually operates. Finally, the few regulations that are public create a confusing and sometimes internally inconsistent thicket of guidelines.

This report sets out to invigorate the public debate on EO 12333 in three ways. First, it reviews several known EO 12333 programs to test the assumption that the NSA's overseas operations have a minimal effect on Americans. Information disclosed both by Snowden and intelligence agencies shows that these operations have implications for Americans' privacy that could well be greater than those of their domestic counterparts. The flow of electronic data is not constrained by territorial borders. The vast majority of Americans — whether wittingly or not — engage in communication that is transmitted or stored overseas. This reality of the digital age renders Americans' communications and data highly vulnerable to NSA surveillance abroad.

Second, the report attempts to distill and make sense of the complex ecosystem of directives, policies, and guidance that form the regulatory backbone of the NSA's overseas operations. Despite a series of significant disclosures, the scope of these operations, as well as critical detail about how they are regulated, remain secret. Nevertheless, an analysis of publicly available documents reveals several salient features of the EO 12333 regime:

- ***Bulk collection of information:*** The NSA engages in bulk collection overseas — for example, gathering all of the telephone calls going into or out of certain countries. These programs include the data of Americans who are visiting those countries or communicating with their inhabitants. While recent executive branch reforms place some limits on how the government may use data collected in bulk, these limits do not apply to data that is collected in bulk and held for a temporary (but unspecified) period of time in order to facilitate "targeted" surveillance.

- ***Treating subjects of discussion as "targets":*** When the NSA conducts surveillance under EO 12333 that it characterizes as "targeted," it is not limited to obtaining communications to or from particular individuals or groups, or even communications that refer to specified individuals or groups (such as e-mails that mention "ISIS"). Rather, the selection terms used by the NSA may include broad subjects, such as "Yemen" or "nuclear proliferation."

- ***Weak limits on the retention and sharing of information:*** Despite recent reforms, the NSA continues to exercise significant discretion over how long it may retain personal data gathered under EO 12333 and the circumstances under which it may share such information. While there is a default five-year limit on data retention, there is an extensive list of exceptions. Information sharing with law enforcement authorities threatens to undermine traditional procedural safeguards in criminal proceedings. Current policies disclosed by the government also lack specific procedures for mitigating the human rights risks of intelligence sharing with foreign governments, particularly regimes with a history of repressive and abusive conduct.

- ***Systemic lack of meaningful oversight:*** Operations that are conducted solely under EO 12333 (i.e., those that are not subject to any statutory law) are not vetted or reviewed by any court. Members of the congressional intelligence committees have cited challenges in overseeing the NSA's network of EO 12333 programs. While the Agency has argued that its privacy processes are robust, overreliance on internal safeguards fails to address the need for external and independent oversight. It also leaves Congress and the public without sufficient means to assess the risks and benefits of EO 12333 operations.

The report concludes with a list of major unanswered questions about EO 12333 and the array of surveillance activities conducted under its rules and policies. While many operational aspects of surveillance programs are necessarily secret, the NSA can and should share the laws and regulations that govern EO 12333 programs, significant interpretations of those legal authorities, and information about how EO 12333 operations are overseen both within the Executive Branch and by Congress. It should clarify internal definitions of terms such as "collection," "targeted," and "bulk" so that the scope of its operations is understandable rather than obscured. And it should provide more information on how its overseas operations impact Americans' privacy, by releasing statistics on data collection and by specifying in greater detail the instances in which it shares information with other U.S. and foreign agencies and the relevant safeguards. Providing this information will not only enhance accountability and public confidence; it will permit an informed public debate and, ultimately, a democratic choice about the ways in which we authorize our government to gain access to our own private data and the data of people around the world. That, in turn, will pave the way for laws and policies that protect both liberty and security.

INTRODUCTION

Documents made public by Edward Snowden show that the National Security Agency ("NSA") conducts surveillance operations outside the U.S. that sweep up massive amounts of electronic communications and private data that are stored or transmitted overseas. In the United States, such disclosures have attracted less attention than the NSA's efforts to gather information inside the country.[2] However, the Agency's overseas surveillance is of a far greater magnitude than the better-known programs that operate at home, and poses risks to Americans' privacy that are likely more serious.

The primary source of guidance for the NSA's overseas surveillance is Executive Order ("EO") 12333, originally issued in 1981.[3] The Order permits intelligence agencies to "collect, retain or disseminate" a wide range of information, subject to procedures to be established by each agency and approved by the Attorney General.[4] The catchall category of information that agencies are permitted to "collect, retain or disseminate" is "foreign intelligence" information, broadly defined to include information "relating to the capabilities, intentions and activities of foreign powers, organizations or persons."[5] In other words, so long as they are operating outside the U.S., intelligence agencies are authorized to collect information about any foreign person — including that person's communications with American friends, relatives, customers, or business associates.

The EO 12333 regime was modified in 2014, when President Obama issued Presidential Policy Directive 28 ("PPD-28") in response to international criticism of U.S. surveillance laws triggered by Snowden's disclosures. For the first time, the U.S. government recognized that foreigners have privacy interests and established minimal rules on how foreigners' data should be handled.

THE HISTORY AND CONTEXT OF EO 12333

EO 12333, the Order under which the NSA conducts most of its overseas surveillance operations, was issued by President Ronald Reagan in 1981.[6] The Order was designed to "enhance" the ability of the intelligence community to acquire foreign intelligence and to detect and counter international terrorism, the spread of weapons of mass destruction, and espionage.[7] While the focus of this report is electronic surveillance, the scope of EO 12333 is not so limited. The Order provides a comprehensive framework for the "conduct of intelligence activities," particularly those undertaken abroad.[8] It sets out the roles and responsibilities of each element of the intelligence community, and authorizes a wide range of intelligence activities beyond electronic surveillance, such as physical searches and mail surveillance.[9]

The Order articulates the need for a "proper balance between the acquisition of essential information and protection of individual interests."[10] It bans certain activities, including assassination,[11] human experimentation,[12] and covert action "intended to influence United States political processes, public opinion, policies, or media."[13] Beyond that, however, as detailed in this report, it includes few restrictions on gathering electronic communications for foreign intelligence purposes.

Although EO 12333, PPD 28, and certain subsidiary guidelines are public, much secrecy and uncertainty remains regarding the legal basis for overseas surveillance programs. Indeed, it may be that some of the regulations in the public domain have been quietly replaced by others that are not publicly available.[14] What is clear — based on publicly available information — is that, despite recent reforms, EO 12333 still allows the NSA to gather vast amounts of digital information about Americans and others around the world. Such information includes not only communications content, but also metadata (such as telephone numbers and the dates, times, and places of communications, which can reveal people's movements and social networks), and other digital information (such as web browser histories and geolocation data). And while there are some rules on how the NSA may use, store, and share such information, there are also numerous loopholes. The lack of robust safeguards is exacerbated by weak external oversight.

This report charts the gaps in the regulation of the NSA's overseas electronic surveillance operations. It begins by compiling publicly available information on some of the operations reportedly carried out under EO 12333, illustrating the ways in which Americans can become entangled in these efforts. Part II of the report gives a bird's-eye view of the legal and policy framework governing overseas surveillance operations. Parts III and IV of the report analyze this framework in detail, focusing on subsidiary regulations that implement the broad guidelines of EO 12333 and PPD-28. Part III shows that there are few substantive constraints on information gathering overseas or on the use of such information once gathered, while Part IV explores the wide latitude that the NSA has to retain and share information. Part V details deficiencies in current oversight mechanisms. Finally, Part VI lists critical questions about the laws and policies governing EO 12333 programs that remain unanswered.

The report concludes that Americans' information is highly vulnerable to NSA surveillance overseas. Accordingly, efforts to protect our privacy that are limited to reining in the NSA's surveillance operations inside the country are fundamentally insufficient.

A CLARIFICATION ABOUT TERMINOLOGY

In our view, "collection," "interception," "acquisition," "gathering," and "obtaining" of information all mean the same thing. However, as explained later in the report, *see infra* Part III.A., "collection" and "interception" are terms of art in the NSA's lexicon, and do not simply mean the acquisition, gathering or obtaining of information. To avoid confusion that might result from the NSA's unusual definitions, this report uses the terms "obtain" or "gather" rather than "intercept" or "collect," except when referring to a government policy or statement that itself uses those terms. We avoid using the term "acquisition" as well because the NSA has relied on the term to draw a false distinction between the ordinary meaning of "collection" and its strained definition of "collection." Moreover, the Foreign Intelligence Surveillance Act — the primary authority for foreign intelligence surveillance on U.S. soil — expressly regulates information "acquisition," and it is unclear how the NSA has interpreted this term.[15]

I. NSA OVERSEAS SURVEILLANCE OPERATIONS

While the full scope of the NSA's overseas operations is far from clear, leaked and declassified documents show that EO 12333 has enabled the gathering of massive amounts of communications as well as information about the relationships and movements of ordinary people worldwide. This section summarizes several of the major overseas surveillance programs reported since 2013 and analyzes the ways in which they may affect Americans' privacy.[16]

A. Intelligence Gathering Operations

The list of the types of information gathered by the NSA is long. It includes: telephone, cell phone, and other voice calls, e-mails, chats, web-browsing history, pictures, documents, webcam photos, web searches, advertising analytics traffic, social media traffic, logged keystrokes, username and password pairs, file uploads to online services, Skype sessions, and more.[17]

Our understanding of the NSA's efforts to gather these types of information is based primarily on the Snowden archive and on documents released in response to recent Freedom of Information Act requests. However, the NSA has conducted overseas surveillance for decades;[18] its historical operations, and almost certainly its current ones, go beyond those revealed in recent disclosures.[19] Even for the activities disclosed by Snowden, information is often fragmentary and incomplete. And, while the government acknowledged some of its domestic surveillance activities after Snowden's disclosures and released additional documents about them, it has been much less forthcoming with respect to its foreign activities. The list below is thus necessarily a sample, focusing on some of the most significant programs that impact Americans' privacy and for which sufficient documentation is available.

1. Telephone Communications and Metadata

The NSA gathers telephone content and metadata transmitted or stored outside the U.S. through a variety of programs.[20] In some countries, the NSA obtains this information in bulk. Under a program codenamed **MYSTIC**, the NSA gathers information about every cell phone call made to, from, and within the Bahamas, Mexico, Kenya, the Philippines, and Afghanistan.[21] Such information includes the numbers dialed and the date, time, and destination of each call. In the Bahamas and Afghanistan, the NSA goes even further: It gathers and stores for thirty days an audio recording of every cell phone call placed to, from, and within these countries using a system codenamed **SOMALGET**.[22] There is no official explanation for why these countries, and not others, were the original targets of the program; in any event, the NSA reportedly intends to expand the program to more countries and may already have done so.[23]

2. Internet Data

The NSA obtains a wide range of information transmitted, stored, and accessed on the Internet. Under a program codenamed **MUSCULAR**, the NSA works with the United Kingdom's intelligence agency, General Communication Headquarters (GCHQ), to tap into the cables connecting internal Yahoo and Google networks to gather information — including e-mail address books and contact lists — from

hundreds of millions of customers.[24] The data is temporarily held in a digital buffer and run through a series of filters to "select" information the NSA wants.[25] In a single 30-day period from December 2012 to January 2013, the NSA "selected" and sent back to its headquarters in Fort Meade over 180 million new records of Internet data from these cables.[26] After these activities were revealed, several major Internet service providers moved to encrypt more of their customers' communications and data.[27] Other reported programs include those codenamed **MONKEYROCKET** and **MADCAPOCELOT**, which gather Internet content and metadata from access points outside the U.S. to aid overseas counterterrorism operations.[28]

Some programs are conducted with the assistance of Internet service providers and other corporate partners. For example, an unnamed corporation provides the NSA with access to Internet metadata transmitted on its networks for a program codenamed **YACHTSTOP**. Another unnamed corporation provided access to Internet and telephone content and metadata for a program codenamed **ORANGECRUSH**, but this may no longer be operational.[29]

3. Webcam Chats

In a program codenamed **OPTIC NERVE**, the NSA collaborated with GCHQ to gather webcam images from video chats among millions of Yahoo users and possibly users of other webcam services.[30] This program swept up the video communications of many U.S. and U.K. citizens, including sexually explicit images. It also used facial recognition to automatically compare faces from the gathered images to the faces of targets. The program was still active as of 2012.

4. Text Messages

The NSA uses a program codenamed **DISHFIRE** to gather the content and metadata of hundreds of millions of text messages from around the globe, and stores the information in a database that is also accessible to the GCHQ.[31] Both the NSA and GCHQ mine the database to obtain, among other things, contact information, location, and credit card details. [32] Specifically, the NSA employs a program codenamed **PREFER**, which appears to analyze automated text messages (such as missed call alerts) to map an individual's social networks.[33]

5. Information from Cell Phone Apps

Cell phone applications — such as Angry Birds and Google Maps — gather, generate, and store information on users' location, age, sex, and potentially other personal information for advertising purposes. These applications are often described as "leaky," because outsiders can covertly access such information with relative ease.

With the assistance of GCHQ, the NSA has reportedly exploited security vulnerabilities in these applications.[34] Google Maps, for example, records where a person has been and where they are planning to go, and the NSA can "clone Google's database" of searches for directions. [35] In order to better target advertising, some cell phone applications create user profiles of characteristics such as ethnicity, political alignment, marital status, and sexual orientation, which may also be available to intelligence agencies.[36]

And when a user uploads a post via the mobile versions of Facebook, Twitter and the like, the NSA can scoop up "address books, buddy lists, phone logs and the geographic data embedded in photos." [37]

While the full scale of the NSA's collection of information from cell phone applications is not known, it reportedly dedicated $767 million to the endeavor in 2007. [38]

6. Cell Site Location Information

Under a program codenamed **CO-TRAVELER**, the NSA has created a database of the location of hundreds of millions of mobile phones outside the U.S.[39] Again, the gathering of such information from the cables that connect mobile networks worldwide relies on the cooperation of telecommunications and Internet service providers.[40] The NSA also tracks the time and duration a mobile phone is switched on, which allows the Agency to determine similar patterns of movement among phones.[41] Such information is used to map relationships between mobile phone users around the world. Users of disposable cell phones and those who switch on their phones for only brief periods of time are singled out for special scrutiny.[42]

Some of the intelligence gathering capabilities described above are enabled by hacking operations. In its bid to gain access to major computer systems and Internet networks, the NSA has gone to great lengths to hack into the computers of system administrators — those who maintain these systems and networks and protect their security.[43] Malicious software that the NSA installs on computers belonging to system administrators enables the Agency to obtain a wealth of sensitive data, including username and password pairs, "network maps, customer lists, [and] business correspondence."[44]

The NSA has also undertaken attacks against users of Tor — an online anonymity tool developed with funding from the U.S. government.[45] In carrying out the attacks, the government claims that its principal interest is in identifying terrorists and organized criminals. But Tor's estimated 2 million users[46] include journalists, human rights workers, activists, researchers, and many others who wish to protect their communications for legitimate reasons.

B. Intelligence Storage, Sharing, and Analysis

All of the information that the NSA obtains is fed into databases that can be accessed and queried by thousands of NSA analysts with relative ease. The largest of these is codenamed **XKEYSCORE**, which receives a "constant flow of Internet traffic from fiber optic cables that make up the backbone of the world's communication network."[47] During a single 30-day period in 2012, at least 41 billion total records were stored on XKEYSCORE. The daily volume of information is so large that it is held on 700 servers in some 150 locations around the world.[48]

With XKEYSCORE, NSA analysts have a universe of information at their fingertips. E-mails, Facebook chats, records of web browsing activities, and even user name and password pairs can be retrieved by completing a fairly basic online search form, in the same way one might pull up cases or articles on a database like LexisNexis.[49] To comply with legal restrictions, analysts are required to fill in a justification for the search. The justifications offered, however, can be very brief,[50] sometimes selected from a

dropdown menu.[51] And while searches establish an audit trail that can be reviewed for legal compliance, there is no public information on how frequently or rigorously these audits are performed.[52]

The information that the NSA stores on its network of databases is accessible to select foreign governments too. The U.S. is part of an intelligence-sharing alliance with Australia, Canada, New Zealand, and the United Kingdom, known as the "Five Eyes." Members gather, analyze, translate, and decrypt communications and related data in their respective parts of the world and share them with their counterparts. The U.K., Canada, New Zealand, and non-Five Eyes partner Germany reportedly have access to XKEYSCORE.[53] The NSA also has shared large volumes of Americans' raw data with Israel.[54]

THE NSA AND ENCRYPTION

Decryption is one type of analysis that the NSA might conduct on data obtained and stored on XKEYSCORE.[55] The Agency's larger efforts to weaken or break widely used encryption technologies pose a further threat to both individual privacy and security.

With the cooperation of some corporate partners, the NSA has inserted secret vulnerabilities (known as backdoors or trapdoors) into a range of commercial encryption software.[56] It also spends more than $250 million a year to "actively engag[e] the US and foreign IT industries to covertly influence and/or overtly leverage their commercial products' designs" in order to make them "exploitable."[57] And it secretly manipulated and weakened an international cryptography standard established by another U.S. government entity, the National Institute of Standards and Technology.[58]

Technology experts and some former national security officials have argued that undermining encryption in these ways actually makes us *less* secure.[59] A respected group of cryptographers has concluded that providing the government with exclusive access to encrypted communications is technically infeasible. Instead, the efforts to facilitate government access specified above will "open doors through which criminals and malicious nation-states can attack the very individuals law enforcement seeks to defend."[60] U.S. demands for encryption backdoors might also trigger a race to the bottom, as other countries' governments (including authoritarian regimes) seek to follow the U.S.'s lead.

C. Impact of EO 12333 Programs on Americans

NSA surveillance conducted under EO 12333 does not only affect foreigners — it also poses major risks to Americans' privacy. As the table on the opposite page shows, the NSA's overseas operations disclosed so far are capable of sweeping up a wide range of electronic communications between Americans and foreigners, and even among Americans themselves. A former State Department official estimates that the communications and data of "millions, or hundreds of millions, of Americans" are swept up under EO 12333.[61]

How 12333 Operations Affect Americans: Mary's Story

PROGRAM	TYPE OF INFORMATION GATHERED	AGENCIES INVOLVED	IMPACT ON AMERICANS
MYSTIC	Records of cell phone calls	NSA	While Mary from Milwaukee is on vacation in the Bahamas, she receives a cell phone call from her daughter, Maria, who confides that she just broke up with her boyfriend. The next day, Mary's bank calls her to inform her about foreign charges on her credit card. The NSA will store information about the time and date of these calls, as well as the phone numbers of Mary, Maria, and the bank.
SOMALGET	Audio content of cell phone calls	NSA	Both calls were received in the Bahamas, so the NSA can access audio recordings for up to thirty days.
CO-TRAVELER	Cell site location information	NSA	Mary attends an Alcoholics Anonymous meeting in Nassau. Her cell phone is switched on, so the NSA could pick up her location, as well as information about cell phones belonging to other participants in that AA meeting.
OPTIC NERVE	Webcam chats and images	NSA, GCHQ	Back in Milwaukee, Mary logs onto a video chat with her husband, who is in Germany on business. The NSA could access stills from the video chat.
MUSCULAR	E-mail address books and contact lists	NSA, GCHQ	Mary is a member of a worldwide Facebook group dedicated to environmental activism, and she regularly e-mails other members of the group using Gmail. The NSA could obtain the Facebook group's membership and Mary's e-mail contacts.
DISHFIRE	Text messages	NSA, GCHQ	The NSA could obtain Mary's text messages with her daughter, the attendees at her AA meetings, her husband, and her environmental activist associates, as well as the text alerts from her bank indicating suspicious activity in her account.
XKEYSCORE	Storage of internet data gathered	NSA, GCHQ, CAN, NZ, GER	Mary's e-mails, Facebook chats, records of web browsing activities, and even user name and password pairs may be stored in this database, which is accessible not only by NSA analysts but also by select foreign counterparts.

NSA surveillance overseas affects even those Americans who do not travel abroad or communicate with people in other parts of the world. The burgeoning popularity of online cloud services, in particular, renders Americans' domestic communications and related data vulnerable to NSA surveillance overseas. A large proportion of American Internet users use "cloud-based" services to communicate.[62] Many of these services store their users' data in data centers around the world, from Singapore to Ireland to Chile. For operational reasons, cloud providers also routinely store backup copies of the same piece of user data in multiple locations.[63] As a result, purely domestic communications increasingly may be stored abroad and thus vulnerable to NSA operations overseas.

Website visits by American users are also vulnerable to surveillance. It goes without saying that visits by American users to foreign websites (for example, the BBC's website with servers in the UK) will be visible to U.S. intelligence agencies operating abroad. But even visits to U.S. websites could be captured. The websites of U.S. news organizations and companies routinely incorporate third party services such as online ads, embedded videos, web analytics, and social plugins.[64] Whenever a user loads a website, connections to these third party services are automatically made in the background — and if any of these connections leaves the U.S., the NSA could learn which U.S. websites the user is visiting. Researchers estimate that 31.7% of visits to popular websites such as Amazon and YouTube contain some foreign component.[65] Such visits could be recorded and stored in XKEYSCORE and other NSA databases.

As the world becomes more interconnected, the NSA's access to Americans' data transmitted and stored overseas will only increase. Americans therefore should be concerned about EO 12333, which, as we show below, grants intelligence agencies extremely broad surveillance powers with few substantive limits and minimal independent oversight.

II. OVERVIEW OF LEGAL AUTHORITIES GOVERNING OVERSEAS SURVEILLANCE

EO 12333 is the primary source of legal and policy guidance for the NSA's overseas electronic surveillance operations, but it does not operate in isolation. Presidential Policy Directive 28 ("PPD-28"), which President Obama issued in January 2014, is one of various policy supplements to the Order, and perhaps the most scrutinized in the wake of Snowden's revelations. The NSA must also comply with all applicable U.S. statutes[66] (in particular, the Foreign Intelligence Surveillance Act) and, of course, the Constitution.

A. EO 12333 and Implementing Procedures

EO 12333 provides general guidance on how intelligence agencies may conduct operations overseas, delegating some of the key details to the agencies. Most notably, the Order states that intelligence agencies are authorized to "collect, retain or disseminate information concerning United States persons" — defined to include U.S. citizens and certain foreigners with significant ties to the U.S. (e.g., U.S. permanent residents) — "only in accordance with procedures established by the head of the Agency concerned and approved by the Attorney General."[67] The Order further stipulates that these procedures "shall permit collection, retention and dissemination" of ten categories of information, including "foreign intelligence or counterintelligence."[68]

The agencies' procedures are thus critical to understanding how electronic surveillance may be conducted under EO 12333. Unfortunately, not all agencies have complied with their duty to establish these procedures. The Department of Homeland Security, the U.S. Coast Guard, the Department of Treasury, and the Drug Enforcement Administration are still "finalizing" their procedures, more than three decades after the issuance of EO 12333.[69] In the meantime, these agencies have stated that they are relying on interim procedures or the guidance of in-house counsel.[70] Moreover, the procedures of the CIA and the Office of the Director of National Intelligence remain classified,[71] and it is not clear whether the publicly available procedures of other agencies — some of which date back to the early 1980s — reflect existing practice.

Keeping in mind possible discrepancies between the published procedures and current practice, this report will focus on EO 12333 procedures that apply to the NSA, which is responsible for most of the electronic surveillance activities described in Part I. In particular, it will focus on two sets of procedures: the 1982 Department of Defense Directive 5240.1-R ("DoD U.S. Persons Procedures"), which governs how information about U.S. persons must be treated by the intelligence components of the Department of Defense, the parent agency of the NSA;[72] and the United States Signals Directive SP 0018 ("NSA U.S. Persons Procedures"), issued by the NSA in 1993 and revised in 2011 to implement the requirements of the DoD U.S. Persons Procedures.[73]

WHO ARE "U.S. PERSONS"?

Certain non-U.S. citizens may be covered by the rules and safeguards that apply to Americans, depending on their physical location and immigration status. In general, a "U.S. person" refers not only to a U.S. citizen, but also a green card holder,[74] an association comprised largely of U.S. citizens or green card holders, and a corporation incorporated in the U.S.[75]

The standard of proof for assessing a target's U.S. person status is whether there is a "reasonable belief" that the person is foreign. In practice, this appears to be a low bar. Analysts have designated targets as foreign based on, at least in part if not entirely, the fact that their e-mails were written in a foreign language; they appeared on the chat "buddy list" of a known foreign national; or their e-mail or social media accounts were accessed via a foreign IP address.[76] Furthermore, the NSA presumes that a person or organization located outside the U.S. is "NOT … a U.S. person UNLESS there is a specific information to the contrary."[77] But tens of millions of Americans speak a foreign language; many more have friends around the world, both offline and online; and millions of Americans travel abroad every year, from where they will access their e-mail, Facebook account, and other websites. The publicly available information about how the NSA determines "foreignness" suggests the Agency may incorrectly tag many Americans as foreign and thereby deny them safeguards to which they are entitled.[78]

B. PPD-28 and Implementing Procedures

On January 17, 2014, in response to the international backlash arising from Snowden's disclosures, President Obama issued PPD-28, a policy directive that supplements the guidelines and procedures under EO 12333. PPD-28 articulates general principles on intelligence gathering, sets limits on how certain categories of communications may be used, and imposes a few restrictions on the dissemination and retention of personal information belonging to foreigners.[79]

Like EO 12333, PPD-28 requires every intelligence agency to establish procedures that implement the general standards set out in the Directive. Significantly, these procedures are supposed to specify the conditions under which personal information belonging to non-U.S. persons may be retained and disseminated.[80] This report will focus on the NSA's PPD-28 Procedures, released in February 2015.[81]

C. FISA and the Constitution

The NSA's overseas electronic surveillance operations must also comply with the Foreign Intelligence Surveillance Act (FISA). As enacted in 1978, the statute largely focused on protecting the communications of U.S. persons located *inside* the country; it contained no limitations on *overseas* surveillance of targets located outside the U.S.[82] In 2008, however, the Act was amended to require intelligence authorities to obtain an order from the Foreign Intelligence Surveillance Court to conduct overseas electronic surveillance that intentionally targets U.S. persons.[83]

It is important to note that this rule would not cover many of the NSA's overseas operations described in Part I, even though they obtain large volumes of electronic communications data concerning U.S. persons. Many of these operations are mass surveillance programs that, by their very nature, do not target particular individuals. For example, a program like SOMALGET, which is capable of sweeping up phone calls between Americans and Bahamians by tapping into Bahamas's communications network, is not subject to FISA's requirement of a court order (provided, of course, that the program is not used intentionally to target U.S. persons).

Finally, regardless of where it takes place, NSA surveillance must be conducted in a manner that is consistent with the Constitution, including the First Amendment rights to free speech and association and the Fourth Amendment right of "the people" to be secure in their "persons, houses, papers and effects against unreasonable searches and seizures." Given the challenges of litigation in this area, however — most notably, the fact that EO 12333 surveillance takes place without any notification of the person or people surveilled, which makes it extremely difficult to establish standing to sue — there is, as yet, no case law on whether programs under EO 12333 meet constitutional requirements.

IS EO 12333 USED TO CONDUCT DOMESTIC SURVEILLANCE?

It is sometimes said that foreign intelligence surveillance conducted overseas is governed by EO 12333, while foreign intelligence surveillance on U.S. soil is governed by FISA. The reality is more complicated.

EO 12333 and its associated directives apply to all foreign intelligence surveillance of electronic communications, not just overseas surveillance.[84] Nevertheless, the Order recognizes the need to comply with relevant U.S. statutes — particularly FISA — and the Constitution.[85] To the extent FISA regulates surveillance that takes place inside the U.S., EO 12333 requires adherence to the statute and to FISA Court orders, in addition to the procedures they stipulate.

Notably, however, FISA does not cover *all* electronic surveillance on U.S. soil to gather foreign intelligence. For example, FISA's definition of "electronic surveillance" would not cover domestic surveillance of radio communications between a person located in the U.S. and someone located overseas, provided that U.S. persons are not intentionally targeted.[86] Thus, FISA does not appear to restrict the NSA's acquisition of cell phone calls between Mary in Milwaukee and her British friend Laura in London as they are being transmitted via radio signals over U.S. soil, as long as Laura is the target.

Some experts suspect that this regulatory loophole allows the NSA to conduct foreign intelligence surveillance activities within the U.S. relying solely on procedures established under EO 12333, which (as we explain later in the report) are less protective of privacy than FISA.[87] This prospect raises grave constitutional concerns. While an analysis of the complex Fourth Amendment issues raised by foreign intelligence surveillance is beyond the scope of this report, we have elsewhere made the case that the Fourth Amendment applies to domestic surveillance of communications between a foreign target and a U.S. person (for instance, the NSA's acquisition of cell phone calls between Mary and Laura).[88] Simply following EO 12333 procedures, which involve no judicial oversight and allow for broad gathering, dissemination, and retention of communications, would not satisfy the Fourth Amendment.[89]

III. GATHERING, PROCESSING, AND USE OF COMMUNICATIONS AND RELATED INFORMATION

Despite recent reforms, the government's authority to gather digital communications and data on a massive scale overseas generally remains intact. Restrictions on the uses of information obtained in bulk and on the ways data may be searched and processed are either too permissive or too malleable. Moreover, it may be possible to evade these restrictions through joint intelligence gathering operations with other countries.

A. A Note on Definitions

Analysis of the gaps in regulation requires an understanding of the meanings that intelligence agencies ascribe to certain terms, which often differ from how these terms are understood in normal parlance. An "Intelligence Law Handbook," disclosed in response to Freedom of Information Act requests, cautions analysts to "adjust" their vocabulary because "[t]he terms and words used in [the DoD U.S. Persons Procedures] have very specific meanings, and it is often the case that one can be led astray by relying on the generic or commonly understood definition of a particular word."[90]

Accordingly, we begin by parsing certain definitions.

1. What Is "Collection"?

The Intelligence Law Handbook indicates that for intelligence agencies housed under the DoD, the act of "collection" is "more than 'gathering' — it could be described as 'gathering, plus…'"[91]

But what additional action is required to complete "collection" depends on which agency you ask and which document you rely on. This makes it difficult to determine which rules, if any, apply when an intelligence agency gathers information. Our analysis shows that there are at least three definitions of "collection":

> 1) the process by which information obtained is rendered "intelligible" to human understanding;
> 2) the process by which analysts filter out information they want from the information obtained; and
> 3) the gathering or obtaining of information (i.e., the ordinary meaning of the word "collection").

Since EO 12333 procedures are triggered only upon "collection," this ambiguity potentially allows the NSA to avoid restrictions simply by categorizing certain information as not having been "collected."

a. DoD: "Collection" is complete only when information is made "intelligible"

The DoD's U.S. Persons Procedures state that:

> Information shall be considered as "collected" only when it has been received for use by an employee of a DOD intelligence component in the course of his official duties … Data acquired by electronic means is "collected" *only when it has been processed into intelligible form.*[92]

It is not immediately clear what kinds of data the DoD would consider "intelligible." Nevertheless, the NSA (a component of the DoD) has explained in its PPD-28 procedures that it might not be possible to process an electronic communication into an "intelligible form" because of "unknown communication methods, encryption, or other methods of concealing secret meaning."[93] While the DoD and the NSA do not always rely on the same definitions, this explanation may provide some clues.

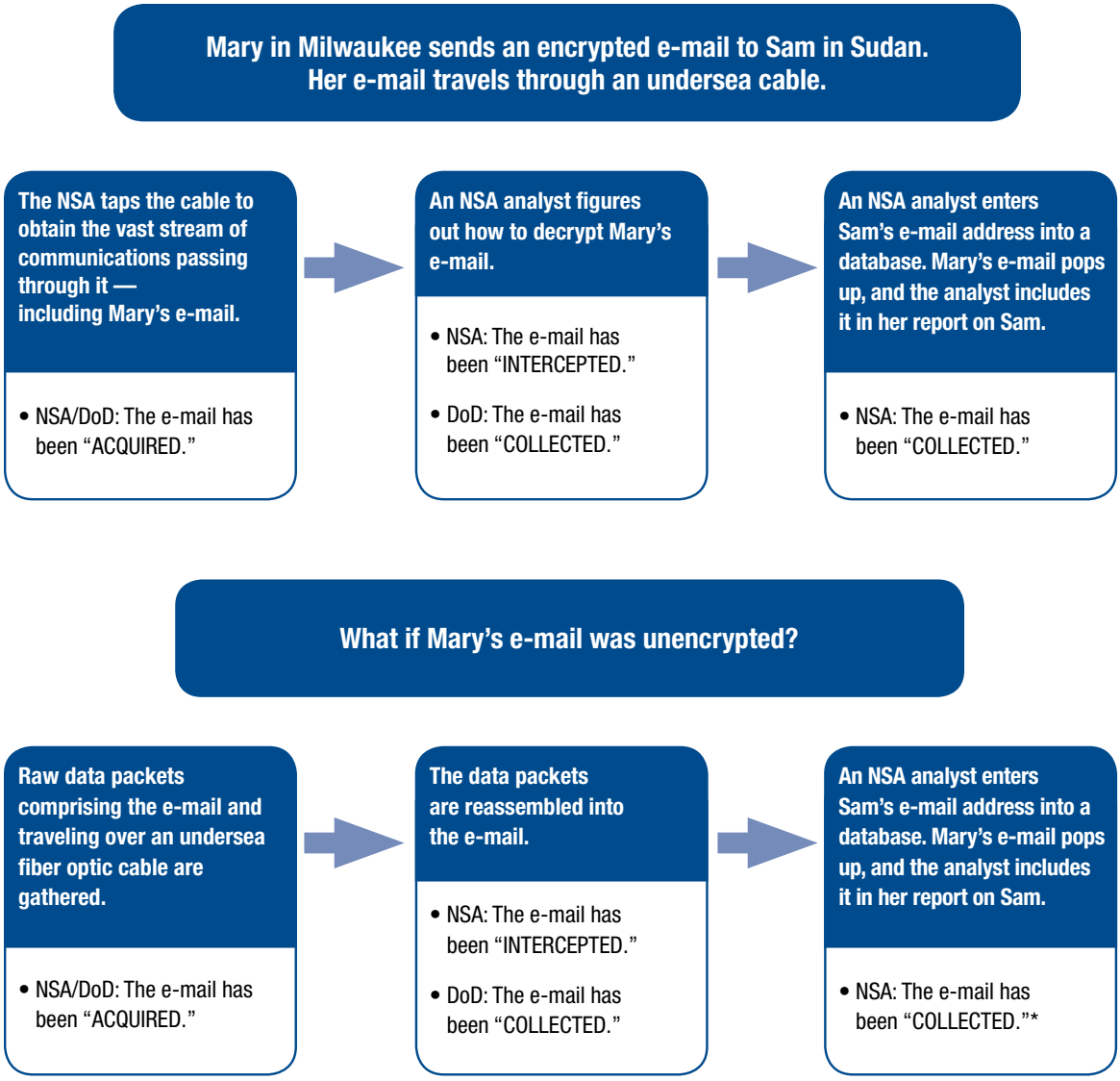
Under this definition of intelligibility, the gathering of encrypted communications would not qualify as "collection." It follows that the gathering of encrypted communications is exempt from the DoD rule that U.S. persons' information may only be "collected" if the information is necessary to fulfill the Agency's functions and belongs to a category that the Agency is permitted to "collect" (e.g., foreign intelligence or counterintelligence).[94] And, since DoD limits on retention apply only to "collected" data, the DoD presumably asserts the authority to store encrypted communications indefinitely — at least until they are decrypted. As encryption becomes increasingly commonplace, such authority would permit the DoD to amass a repository of global communications that it can access, analyze, and share at a later time.

This interpretation of intelligibility might even exclude certain acquisitions of plain text communications from the definition of "collection." Communications may be broken up into a series of data packets when they are stored on a server or in transit from one server location to another. When the NSA gathers information electronically, it could be gathering and storing these data packets, which would be "unintelligible" to the human eye until subsequently reassembled by a processing system into the original communication. As a result, the NSA might consider that "collection" has not taken place until the communication has been reassembled, even though fragments of it have been gathered and stored.

b. NSA: "Collection" is complete only when intelligible information is analyzed

Although the NSA operates under the DoD's authority, its U.S. Persons Procedures define the relevant terms more narrowly, suggesting that even less information comes under protective procedures. The NSA uses the term "interception" to describe what the DoD procedures call "collection." In other words, when the NSA decrypts or otherwise processes the communications it gathers into "intelligible form," it has only "intercepted" such data.[95]

Under the NSA's procedures, "[c]ollection" does not take place until an analyst "intentional[ly] task[s] or select[s]" a communication "for subsequent processing aimed at reporting or retention as a file record."[96] Such tasking or selection is performed when an analyst applies a selector term, such as a telephone number or e-mail address, to one of the NSA's databases.[97]



*It may be that the analyst's search triggers both the reassembly process and its subsequent display. As a result, the analyst may have simultaneously intercepted and collected Mary's e-mail when she conducts a search of Sam's e-mails.

Under both the DoD and NSA definitions, the logical inference is that the Agency's privacy safeguards and other internal restrictions are triggered only when gathered data has been processed in some way.[98] As a result, there is potentially no limit on the prior gathering of information concerning U.S. persons or its storage as raw, "unselected" data.

This gather-it-all approach is not simply theoretical. Recall that, under the SOMALGET program, the NSA is recording every cell phone conversation to, from, and within the Bahamas and Afghanistan.

Under its U.S. Persons Procedures, the NSA could take the position that it has not "intercepted" many of the conversations obtained simply because they are encrypted or otherwise "unintelligible" (however defined). The Agency could also argue that it has not "collected" these conversations because they have not been "selected" for intelligence analysis or long-term retention.[99]

The mere fact that data obtained by the NSA are being held in a government-controlled repository has significant implications for privacy. They contain personal and sensitive data belonging to millions of innocent citizens worldwide, including U.S. persons. Such data is vulnerable to mishandling or abuse. Furthermore, any lapses in the security of the buffer could expose such data to criminals, hackers, and foreign adversaries.

c. PPD-28: "Collection" as information gathering?

PPD-28 deepens the "collection" conundrum: There is some indication that the Directive relies on the common sense meaning of the word. PPD-28 establishes general principles on intelligence "collection," and also introduces the concept of "bulk collection." PPD-28 states that:

> References to signals intelligence collected in "bulk" mean the authorized collection of large quantities of signals intelligence data which, due to technical or operational considerations, is acquired without the use of discriminants (e.g., specific identifiers, selection terms, etc.).[100]

While PPD-28 does not impose specific constraints on "bulk collection," it provides that there are only six permissible "uses" of "bulk collect[ed]" data.[101] The NSA presumably is only allowed to process and analyze such data in ways that are consistent with these six uses. But if the definition of "collection" is information analysis rather than information gathering, then PPD-28 simultaneously contemplates the "bulk analysis" of data and the imposition of limitations on such analysis. To avoid this contradiction, the word "collection" under PPD-28 logically must be understood to mean information gathering. (As a result, we later discuss PPD-28's principles on "collection" as principles on information gathering.)

2. "Bulk" versus "Targeted"

The NSA uses the terms "bulk" and "targeted" to describe its programs. A common sense reading of these terms would suggest that "bulk" refers to gathering information on a large scale and/or indiscriminately, while "targeted" refers to the gathering of information about specific persons or entities of foreign intelligence interest. As explained below, however, the NSA has a very broad understanding of the meaning of "targeted" and gathers information in massive quantities even in its so-called targeted programs. The Agency's information gathering strategies include:

- **Gathering information *en masse* for storage:** The NSA engages in the broadest possible form of surveillance when it gathers information without the use of search terms, and stores *all* of this information in databases that may be searched at a later time.[102] The government takes the position that only this surveillance strategy amounts to information gathering in "bulk."

- **Gathering information *en masse* to facilitate processing:** The NSA may gather information *en masse* and hold it temporarily in a buffer or database in order to run search terms that determine what part of the information it will keep. It is unclear how long the Agency may hold on to such information before it is considered "collected" under these definitions. Even though such surveillance allows the government to keep and analyze vast stores of information that have been derived from an even larger pool of temporarily obtained data, PPD-28 considers this approach to be "targeted."[103]

- **Applying search terms at the point information is gathered:** Finally, the NSA may use search terms at the point information is gathered. Under PPD-28, such surveillance also would be considered "targeted." While this technique is by definition more selective than the two outlined above, it may not be as limited as it appears at first blush. As we explain below, the permissible search terms are not limited to specific individuals or organizations, and could be quite broad.

B. Restrictions on Information Gathering and "Collection"

Existing rules for gathering or "collecting" information — whether general principles that apply to surveillance across the board, rules on information searches, or rules on the uses of information gathered — are unlikely to impose meaningful restrictions on the NSA's ability to amass a vast repository of electronic communications and data.

1. General Principles on Gathering Information

PPD-28 establishes four principles to govern "collection" (which we interpret to mean "gathering," as discussed above),[104] but these are formulated in such a general way that they avoid dealing with the most controversial aspects of the NSA's surveillance activities.

First, the Directive requires intelligence gathering to be authorized by "statute or Executive Order, proclamation, or other Presidential directive,"[105] but provides no further information about how this principle will be implemented in practice, and no clarification as to any constitutional or other legal limits on either executive or legislative authority.

Details about how intelligence agencies will honor their commitment to legality are critical given the executive branch's history of excessive secrecy. For example, documents disclosed by Snowden showed that the NSA covertly gathered Americans' telephone records in bulk for years under Section 215 of the PATRIOT Act. This was seemingly at odds with the text of the law at the time, which permitted the government to obtain a secret court order requiring third parties to hand over only those records deemed "relevant" to an international terrorism, counterespionage, or foreign intelligence investigation.

Second, the Directive states that "[p]rivacy and civil liberties shall be integral considerations in the planning of U.S. signals intelligence activities," that "[s]ignals intelligence shall be conducted exclusively where there is a foreign intelligence or counterintelligence purpose," and that the U.S. shall not collect signals intelligence "for the purpose of suppressing or burdening criticism or dissent,

or for disadvantaging persons based on their ethnicity, race, gender, sexual orientation, or religion."[106] ("Signals intelligence," abbreviated "SIGINT," is intelligence derived from electronic signals and systems;[107] PPD-28 focuses on SIGINT activities designed to acquire communications or information about communications.[108]) While these general statements reflect a commitment to constitutional norms, it is not clear how they are operationalized or enforced. In particular, the anti-discrimination pledge does not clarify whether the expression of beliefs or views many regard as extreme might be a valid consideration in decisions to initiate or increase surveillance.[109]

Third, the Directive provides that "foreign private commercial information or trade secrets" may be gathered only to protect the national security of the U.S., its partners, or its allies, and not "to afford a competitive advantage to U.S. companies and U.S. business sectors commercially."[110] This assurance, however, contains critical loopholes. The Directive notes that certain economic purposes, such as "identifying trade or sanctions violations or government influence or direction," do not constitute "competitive advantage."[111] Amid reports that the NSA has been spying on Petrobas, a Brazilian oil company, and SWIFT, a money transfer service, the Director for National Intelligence has defended such surveillance as a means of providing the U.S. and its allies "early warning[s] of international financial crises" and "insight into other countries' economic policy or behavior which could affect global markets."[112]

Taken to their logical conclusion, these justifications could render business dealings that contemplate *any* degree of government involvement vulnerable to NSA surveillance. To be sure, there are legitimate national security reasons for obtaining commercial or financial information — for example, to monitor fraud and other criminal wrongdoing, or to detect foreign industrial espionage. But the fine line between national security and industrial espionage requires nuanced policy calculations about the costs and benefits of commercial surveillance that go beyond general assertions of "government influence."[113]

Finally, the Directive requires intelligence gathering to be as "tailored as feasible,"[114] but again offers no specifics regarding implementation. Notably, the tailoring principle is a longstanding cornerstone of the DoD and NSA U.S. Persons Procedures on "collection."[115] However, given how much information the NSA gathers, processes, and analyzes on a daily basis despite the pre-existing tailoring directive, it is questionable whether this emphasis on using the "least intrusive means" of surveillance has much practical impact.

2. Restrictions on the "Bulk" Gathering of Data

"Bulk" data gathering, as the government defines it, is inherently unrestricted at the point such data is obtained. In other words, no filters are used, and entire streams of communications and data are swept up and retained in government databases. PPD-28, however, provides that the data gathered in bulk may be used only to detect and counter: (1) threats of espionage and other activities directed by foreign powers against the U.S.; (2) terrorist threats to the U.S.; (3) threats to U.S. posed by weapons of mass destruction; (4) cybersecurity threats; (5) threats to U.S. or allied armed forces; and (6) transnational criminal threats.[116]

As a threshold matter, restrictions on the *uses* of information gathered in bulk are too little, too late. The notion that the "mere" gathering of information poses negligible harm to privacy has been rejected in other legal contexts. In a decision declaring that the NSA's bulk collection of telephone records was illegal, the U.S. Court of Appeals for the Second Circuit held that the plaintiffs had standing to challenge the program even if the government had not reviewed or analyzed their data.[117] The court found that data gathering, without more, would amount to a "seizure" under the Fourth Amendment if there were a reasonable expectation of privacy in the information.[118] Implicit in the court's reasoning is the recognition that there are "separate privacy interest[s] not just in how the government *uses* our data, but in the government's [gathering] of our data in the first place."[119]

The effectiveness of the "gather everything, search later" approach is also questionable. Two independent reviews of the bulk domestic telephone records program could not identify a single instance where it had contributed essential information to a counterterrorism investigation.[120] The effectiveness of other large-scale surveillance programs, both in the U.S. and abroad, remains an open question. Only the intelligence community has the information necessary to conduct a comprehensive review of whether the yield from mass surveillance is commensurate with the privacy, financial, diplomatic, and other costs, or whether necessary intelligence could have been obtained using more focused techniques. But, as the Privacy and Civil Liberties Oversight Board has noted, the intelligence community is not in the habit of conducting these types of evaluations, despite the urgent need for them.

In any case, some of PPD-28's use restrictions contain troubling ambiguities. In particular, the NSA's ability to use bulk-gathered information to thwart "terrorist" and "cybersecurity" threats revive highly contentious debates about legitimate counterterrorism and cybersecurity purposes. In the absence of further limitation, terrorism is neither a well-defined nor stable concept, and is prone to varying interpretations. There are multiple definitions of terrorism and terrorism-related offenses in U.S. law; some of these are broad enough to encompass seemingly ordinary crimes[121] and even First Amendment activity.[122] Recent developments also raise concerns about how expansively cybersecurity threats will be interpreted. For example, U.S. intelligence agencies have conducted large-scale, warrantless surveillance of Americans' international Internet traffic,[123] and created vulnerabilities in Internet products and services,[124] in the name of a broad range of "cybersecurity" purposes.

3. Rules Governing "Targeted" Surveillance

Even when the NSA uses search terms to gather or analyze information, the rules on how such searches may be conducted still allow the Agency to amass large volumes of private communications and data that may have little to do with the target it is pursuing.

NSA analysts may search for data or search existing stores of data using search terms based on:

1) "the identity of the communicant or the fact that the communication mentions a particular individual";
2) "the content of the communication" (for example, searches for keywords); and
3) the "enciphered" nature of the communication (i.e., a communication that is encrypted or thought to contain secret meaning).[125]

Certain limitations apply when search terms are likely to retrieve U.S. persons' data, and PPD-28 created some protections for non-U.S. person searches as well — but these do not appear to impose major constraints. Moreover, as discussed below, the targeting of communications based on their "enciphered" status is highly problematic.

a. Limits on searches implicating U.S. persons' information

Under the NSA's U.S. Persons Procedures, those content-based searches and searches designed to find encrypted communications that are "reasonably likely to result in the INTERCEPTION of communications to or from a U.S. PERSON" may be performed only if "there is reason to believe that FOREIGN INTELLIGENCE will be obtained."[126] Additionally, such searches "shall be designed to defeat, to the greatest extent practicable under the circumstances, the INTERCEPTION of those communications which do not contain FOREIGN INTELLIGENCE."[127]

But the effectiveness of the "foreign intelligence" limitation is undermined by the term's remarkably broad definition. As explained above, "foreign intelligence" includes any information "relating to the capabilities, intentions and activities of foreign powers, organizations or persons … [and] international terrorist activity"[128] — i.e., any information concerning any activity of any foreign person. NSA training slides indicate that content-based search terms can cover topics as wide ranging as "nuclear proliferation, oil sales, [and] economics."[129] These types of search terms would sweep up massive amounts of U.S. persons' communications, including casual conversations about U.S. foreign affairs.

The General Counsel of the Office of the Director of National Intelligence (ODNI) has countered that intelligence agencies do not "decide on [their] own which conversations to listen to, nor d[o] [they] try to collect everything."[130] Instead, search terms are keyed to foreign intelligence priorities (also referred to as "authorized foreign intelligence requirements"[131]) identified through an "extensive, formal interagency process."[132] Search terms also must "be reviewed and approved by two persons" before being entered into the NSA's databases.[133]

Internal processes, however, are no substitute for substantive limits. The nation's experience with intelligence abuses has shown time and again that reliance on purely internal oversight does not adequately protect privacy and civil liberties.[134]

Moreover, it does not appear that the agencies' internal processes have succeeded in distilling "foreign intelligence" down to narrow topics. While the list of intelligence priorities, memorialized in the National Intelligence Priority Framework,[135] is classified, the ODNI claims that "much of it is reflected annually in the DNI's unclassified Worldwide Threat Assessment."[136] The Assessment typically identifies an extensive list of general topics (e.g., weapons of mass destruction, cybersecurity, transnational organized crime) and even entire countries (e.g., Egypt, China, Yemen) as areas of concern.

b. Limits on searches affecting non-U.S. persons

PPD-28 extends some of these limits to searches that affect non-U.S. persons. Both the DoD's and NSA's PPD-28 procedures provide that they will use, "wherever practicable," search terms that focus

on "specific foreign intelligence targets" (like "specific, known international … terrorist group[s]") or "specific foreign intelligence topics" (like "the proliferation of weapons of mass destruction").[137] The recognition that surveillance of foreigners should not be unlimited is a step towards bringing the U.S. closer to compliance with its obligations under human rights law, such as those contained in the United Nations International Covenant on Civil and Political Rights (ICCPR), to which it is a party.[138] Nonetheless, the efficacy of these limits is questionable.

For one thing, search terms based on "specific foreign intelligence targets" would not be limited to phone numbers or e-mail addresses associated with those targets, but could also include the targets' names. Any communications whose content simply mentions those names are therefore subject to surveillance. In cases where the targets are well-known subjects of public discussion — such as "Osama bin Laden" or ""ISIS" — surveillance is highly likely to capture large numbers of communications between ordinary citizens who are simply discussing current events. Moreover, the broad definition of "foreign intelligence" means that search terms based on "specific foreign intelligence topics" could capture a wide range of innocuous information. As discussed above, these need not relate to a particular individual or group, but can encompass entire subject matters of general interest.[139] Finally, the caveat that these limits should be applied "wherever practicable" leaves a great deal of discretion with an agency that is subject to minimal oversight outside the executive branch.

c. Searches for "enciphered" communications

The practice of gathering communications simply because they are "enciphered" is likely to capture reams of entirely routine personal communications that have nothing to do with terrorism or national security.[140] "Enciphered" communications commonly refers to encrypted communications, but could also refer to any communication that conveys "secret meaning."[141] It's not just "bad guys" who use encryption and other methods to convey secret meaning. Journalists, dissidents, and human rights defenders are among some of the individuals who rely on encryption and secret meaning to protect their identities and communications with sources, clients and activists.[142] Encryption, in particular, is going mainstream. Technology companies from Microsoft to Google to Apple are moving to encrypt data created and transmitted using their devices and services as a matter of routine.[143] Indeed, the NSA itself recognizes the prevalence of encryption today:

> Twenty years ago, the fact that communications were encrypted meant that they were very likely to contain foreign intelligence, because only governments or other important targets had the resources to purchase or develop and implement encrypted communications. Today, anyone who uses the Internet can access web pages via the strong commercial encryption provided by HTTPS, and companies of all sizes can implement virtual private networks (VPN) to permit their employees to access sensitive or proprietary company data securely via an Internet connection from anywhere in the world.[144]

In light of the growing use of encryption, not only by those who are seeking to secure sensitive information but also by regular Internet users, the NSA's insistence on being able to gather all encrypted communications is anachronistic.

In sum, the use of search terms to "target" surveillance gives the illusion that the NSA's gathering and processing of information is carefully tailored to specific operational goals and needs. But publicly available data suggests otherwise. The NSA's large-scale sweep of address books and contact lists under the MUSCULAR program, for example, would fall within its definition of "targeted" because the data is sent through a series of filters to "select" the information the NSA wants. Nonetheless, the Agency obtained hundreds of millions of new records in the span of three months.[145] Characterizing this operation as "targeted" obscures the true scope of information swept up by such surveillance activities.

C. Joint Intelligence Gathering Operations

Joint intelligence gathering operations are another potentially vital source of information for the NSA. While there appears to be some restriction on *sharing* intelligence with other governments (discussed in Part IV.D below), there are no publicly available documents setting forth any limitations on inter-government cooperation to *gather* intelligence.

Documents from the Snowden archives raise concern about the extent to which intelligence gathering arrangements are used to circumvent U.S. privacy protections. For example, does the U.S. rely on partner countries to conduct surveillance prohibited under its own laws? A senior intelligence official has assured Human Rights Watch and the ACLU that U.S. intelligence agencies cannot *ask* foreign partners to collect information that the U.S. is legally prohibited from collecting, but has acknowledged that they can *accept* information that the U.S. could not legally gather on its own.[146] The distinction may be illusory, however, as our closest partners are likely aware of what information we are hoping to gather. The risk is that the U.S. could use this avenue as an end run around the limitations on its own authority. More information is needed on how this principle works, and whether greater checks and balances are needed to ensure that the U.S. does not rely on joint intelligence gathering operations to circumvent domestic privacy and civil liberties safeguards.

The analysis above demonstrates that existing restrictions on the gathering, processing, or use of data under EO 12333 are undermined by counterintuitive definitions, ambiguity, and loopholes. The default limit on the NSA's authority to gather information is EO 12333's expansive definition of "foreign intelligence," and additional limits imposed on the use of information obtained in bulk are unclear. Moreover, even these constraints are undermined by the Agency's definitional maneuvers — defining "collection" to mean analysis and describing as "targeted" the gathering of hundreds of millions of pieces of data. Joint intelligence operations can further eviscerate these limits. Under this scheme, private communications — of both Americans and foreigners — are vulnerable to a wide range of NSA surveillance operations.

IV. RETENTION AND SHARING OF COMMUNICATIONS AND RELATED INFORMATION

Existing rules governing the retention of information are similarly permissive, allowing the NSA to maintain vast stores of private communications and data. The privacy risk created by such large databases of information is compounded by lax dissemination guidelines, which give the Agency wide latitude to share such information with other U.S. agencies and even foreign governments.

A. Data Retention

The rules governing the retention[147] and dissemination of U.S. persons' information obtained under EO 12333 are set forth in the agencies' U.S. person procedures.[148] Under the DoD and NSA's U.S. Persons Procedures, U.S. persons' information may be retained for up to five years. In December 2014, Congress — which had not previously attempted to regulate EO 12333 surveillance — took the unusual step of codifying this limitation.[149] PPD-28 establishes the same retention period for non-U.S. persons' information.[150]

The five-year limit under the agencies' procedures and PPD-28 is subject to numerous exceptions.[151] Recently, Congress made minor modifications to some of these exceptions and established reporting requirements on their use; it directed intelligence agencies to bring their internal procedures in line with these changes within two years of enactment. The legislation nonetheless allows intelligence agencies to keep sensitive personal details in their databases for longer than five years if such information falls within any of the following categories:

1. ***Foreign intelligence or counterintelligence:*** The communication constitutes foreign intelligence, counterintelligence, or information "necessary to understand or assess foreign intelligence or counterintelligence."[152] Here, again, the broad definition of "foreign intelligence" comes into play.

2. ***Evidence of a crime:*** The communication is "reasonably believed" to constitute evidence of a crime "and is retained by a law enforcement agency."[153] There appears to be no restriction on the types of crimes that may trigger this exception; it applies to minor misdemeanors and violent felonies alike.

3. ***Communications that are enciphered or have secret meaning:*** The communication is "enciphered or reasonably believed to have a secret meaning."[154] The NSA's ability to retain encrypted communications indefinitely is particularly concerning given that encryption is becoming widespread, as discussed above.

4. ***Communications between non-U.S. persons:*** All parties to the communication are "reasonably believed to be non-United States persons."[155] As discussed earlier, the mechanism for making this determination is notably imprecise. On the other hand, the retention of such communications is limited by PPD-28's restrictions on the retention and dissemination of non-U.S. persons' information, which are discussed below.

5. ***Protection of imminent threat to human life:*** The communication is "necessary to protect against an imminent threat to human life."[156] This formulation is narrower than the analogous standard under the NSA U.S. Persons Procedures, which allows the NSA to retain information that is "*pertinent to* a *possible* threat to the safety of any person or organization."[157] Congress has also established reporting requirements when an intelligence agency avails itself of this exception. In particular, "the nature of the threat and the information to be retained" must be reported to the congressional intelligence committees "not later than 30 days" after the date such retention is extended.

6. ***Technical assistance:*** The information is "necessary for technical assurance or compliance purposes" — for example, compliance with a court order or discovery obligation. When such information is accessed and for what purposes must be reported to the congressional intelligence committees "on an annual basis."[158]

7. ***National security:*** The information has been approved for further retention by the relevant intelligence official based on a determination that "retention is necessary to protect the national security of the United States."[159] This formulation is arguably more restrictive than the analogous standard under the NSA U.S. Persons Procedures, which allows retention longer than five years if the Signals Intelligence Director determines that retention is "required to respond to authorized FOREIGN INTELLIGENCE requirements."[160] While national security and foreign intelligence often overlap, the latter encompasses a broader range of interests.[161] In addition, reporting requirements apply when this exception is invoked.[162] Despite these added constraints, the exception remains potentially quite broad, as "national security" is an amorphous concept that may be given a range of interpretations.

As for non-U.S. persons, the executive branch recognized for the first time in PPD-28 that intelligence activities must "include appropriate safeguards for the personal information of all individuals, regardless of the nationality of the individual to whom the information pertains or where that individual resides."[163] The Directive thus permits intelligence agencies to retain and disseminate information concerning non-U.S. persons only when "comparable information concerning U.S. persons" would be legally permitted.[164] Given the weakness of the data retention rules for Americans, however, PPD-28 largely preserves the NSA's ability to retain large amounts of sensitive and possibly innocuous information concerning non-U.S. persons.[165]

B. NSA Sharing of Americans' Information

Much of the personal information that the NSA stores may also be accessible to other U.S. government agencies and even some foreign governments. At the time of publication, the White House and the Office of the Director of National Intelligence were reportedly in the process of establishing procedures that will expand intra-government access to raw data gathered by the NSA, including communications to, from, and about U.S. persons.[166] This change could effectively moot existing limitations. In any event, the key current limitation on the NSA's ability to disseminate intelligence reports containing U.S. persons' information — that such information be "necessary to understand ... *FOREIGN INTELLIGENCE* information or assess its importance" — is, for the reasons described above, fairly porous.[167] As a result, regardless of whether the rules are amended to allow greater sharing of raw data

with other agencies, the amount of U.S. persons' information that could be included in intelligence reports is significant.

The NSA U.S. Persons Procedures specify categories of information that the Agency shares under this standard, and some of them could be interpreted quite broadly.[168] For instance, U.S. persons' information may be shared if "pertinent" to a "possible threat" to the safety of "any person or organization," no matter the magnitude of the threat or the degree of probability.[169] While a common sense reading of this language might suggest a reasonably high bar, the counterintuitive reading that the NSA has given to other terms (such as "collect" or "relevant," discussed above[170]) gives cause for concern.

This "foreign intelligence" standard also permits the dissemination of information indicating a U.S. person's involvement in criminal activity. Sharing is not limited to the most serious crimes, or crimes related to terrorism, espionage or national security.[171] The NSA also may share information that pertains to a laundry list of ordinary crimes, including perjury and making false statements in "formal reports or applications" to the government,[172] illegal "tampering with, or unauthorized access to, computer systems" (apparently even if it is not "likely to affect" national security),[173] and drug possession above certain limits.[174]

The dissemination of such information to law enforcement agencies potentially enables the circumvention of the Fourth Amendment in criminal cases. In general, if law enforcement agents conduct electronic surveillance without a warrant, the government cannot use the fruits of that surveillance as evidence in a criminal prosecution. Communications obtained under EO 12333, however, may be gathered through mass, even indiscriminate, surveillance. The NSA's ability to share such information with U.S. law enforcement could therefore create an end run around the strict, constitutionally mandated rules of evidence gathering that govern ordinary criminal investigations. This threat is not simply theoretical. The Drug Enforcement Administration (DEA) has reportedly obtained intelligence information from the NSA to launch criminal investigations, and routinely "recreates" the investigative trail to obscure the original source of the information.[175] To make matters worse, the government has stymied legal challenges to this practice by refusing to disclose the origin of evidence derived from EO 12333 operations even in criminal cases where it is used.[176]

The lax sharing rules also create a risk of mission creep. The availability of a rich trove of intelligence for a wide range of criminal prosecutions — with no requirement to obtain a court order for access — incentivizes reliance on foreign intelligence gathering to conduct domestic law enforcement operations, This in turn jeopardizes longstanding constitutional protections for criminal suspects and defendants. The lack of transparency about the extent of such use only compounds the problem.

C. Sharing of Non-U.S. Persons' Information

Although PPD-28 requires the intelligence community to provide comparable restrictions on how U.S. and non-U.S. persons' information are handled, the agencies' rules implementing PPD-28 are considerably looser when it comes to sharing non-U.S. persons' information. The NSA is generally permitted to share non-U.S. persons' information for purposes similar to those outlined for U.S. persons. But the required nexus between the information in question and the relevant purpose is less strict:

When May U.S. Persons' Information Be Shared?[177]	When May Non-U.S. Persons' Information May be Shared?[178]
The information is *necessary to understand* the foreign intelligence information or assess its importance.	There is *some indication* that information about *"routine activities… is related* to an authorized foreign intelligence requirement."
The information *indicates* that the U.S. person may be engaged in international narcotics trafficking activities, or is evidence that *the individual may be involved in* a crime that has been, is being or is about to be committed.	The information is *related to* a crime that has been, is being, or is about to be committed.
The information *indicates* that the identity of the U.S. person is *pertinent* to a possible threat to the safety of any person or organization.	The information *indicates* a possible threat to the safety of any person or organization.

Since the issuance of PPD-28 in 2014, the NSA states that it does not share non-U.S. persons' information solely because of the person's foreign status;[179] however, the three independent bases for sharing are potentially quite broad. The second and third of these are addressed in the previous subsection. As for the first basis, which allows the Agency to share "information about the routine activities of a non-U.S. person" when there is "some indication" that it is related to an "authorized foreign intelligence requirement,"[180] Part III.B.3.a explains that foreign intelligence requirements may be framed as broadly as "cybersecurity" or "Yemen."

Accordingly, even though the NSA would not be able to disseminate e-mails between French students living abroad simply because they are French, their e-mails may still be fair game if they express alarm at the Office of Personnel Management security breach, or debate the legality of U.S. drone strikes in Somalia.

D. Dissemination of Personal Information to Foreign Governments

Until recently, there has been virtually no public information about when and how intelligence agencies share information with foreign governments. A policy directive recently released by the Director of National Intelligence and a leaked Memorandum of Understanding between the United States and Israel raise questions about whether intelligence agencies give sufficient consideration to the risk that information provided to a foreign government could contribute to human rights abuses and whether they contain appropriate privacy safeguards.

1. Limits on Purposes for which Information may be Shared

Under the March 2013 Intelligence Community Policy Directive 403 on "Foreign Disclosure and Release of Classified National Intelligence" ("ICD 403"), information may be provided to a foreign government when it is: 1) consistent with U.S. law; 2) clearly in the national interest; and 3) "intended for a specific purpose and generally limited in duration."[181] A supplement to the Directive explains that, under these criteria, intelligence may only be considered for disclosure or release if doing so 1)

would be "consistent with U.S. foreign policy and national security goals and objectives"; and 2) "can be expected to result in an identifiable benefit to the U.S."[182] It also prohibits disclosures that would be contrary to U.S. law or treaties.

In cases involving communications concerning U.S. persons, the supplement indicates that U.S. person information may be shared only if authorized by, and in accordance with relevant procedures under, EO 12333. As explained earlier, however, the categories of information that may be shared under these procedures are prone to expansive interpretation.[183] When it comes to non-U.S. persons, the picture is less clear. In theory, intelligence agencies must comply with PPD-28, which extends to non-U.S. persons EO 12333's protections for U.S. persons.[184] The supplement, however, was issued before PPD-28 (although it was made public only recently) and has no mention of any equivalent protections for non-U.S. persons.

2. The Requirement of "Adequate Protection"

The Directive also requires an assessment of whether the foreign government recipient is "likely" to give the information shared "adequate protection."[185] Under the supplement, adequate protection includes "confidence" that the recipient will not disclose the information, has the "capability and intent to provide U.S. intelligence substantially the same degree of protection provided it by the U.S.," will not use the information "for other than the stated purpose," and that the information "is not likely to be used by the recipient in an unlawful manner or in a manner harmful to U.S. interests."[186]

The last provision could serve as a basis for refusing to share information when there is a possibility that it will be used to violate human rights. Protecting and promoting human rights is obviously a goal of the United States, which is party to many of the major human rights treaties. Given the security focus of those who make decisions about sharing, however, it is also possible that a general reference to "U.S. interests" — as opposed to an explicit requirement to consider the human rights impact of sharing information — will be insufficient to ensure proper consideration of these consequences.

3. Intelligence Sharing MOU with Israel: A Case Study

A leaked Memorandum of Understanding (MOU) between the NSA and Israel's signals intelligence agency is illustrative of the potential privacy and human rights risks of sharing arrangements. The MOU relates to the sharing of raw intelligence which has not been reviewed by U.S. analysts and not been scrubbed of U.S. persons' information, safeguarding it in the following ways:

- **Limitation on use of shared intelligence:** Israel is not permitted to use any intelligence data provided by the NSA to "intentionally intercept the communications to, from, or about a U.S. person."[187]

- **Deletion or masking of U.S. persons' information:** Israel may only disseminate foreign intelligence information concerning U.S. persons in a manner that does not identify the U.S. person, whether "by name [or] by context."[188]

- **Destruction of data identifying U.S. persons:** The original files containing the identities of U.S. persons (i.e., the unmasked data) must be "retained for no more than one year."[189]

- **Training and audits:** The NSA provides "annual review and training" to Israeli intelligence officials on the procedures for handling U.S. person information, and "[r]egularly reviews a sample of files transferred to [Israeli intelligence] to validate the absence of U.S. persons' identities."[190]

- **Reporting requirements:** If Israel detects the identity of a U.S. person in raw intelligence data provided by the NSA, it must provide a "written report … on a quarterly basis, detailing the circumstances of those instances."[191] Israel must also inform the NSA immediately upon the discovery of "inadvertent intercept of U.S. person communications where a selector that is believed to belong to a valid foreign target is subsequently found to belong to a U.S. person."[192]

It is unclear why the NSA does not implement safeguards for U.S. persons' information itself before transmission and instead relies primarily on a foreign intelligence service to perform this function, which is so critical to protecting Americans' privacy.

Furthermore, the MOU is silent with respect to information concerning non-U.S. persons. The Director of National Intelligence has stated that the U.S. "takes steps designed to ensure that any disclosure to a foreign government, or other entity, serves a legitimate and authorized purpose and will not be used to, among other things, suppress human rights activities or harm human rights activists."[193] But none of the publicly available directives explains how intelligence agencies take into account the impact of intelligence sharing on the human rights of non-U.S. persons. The lack of transparency raises concern that shared information could be used to repress, censor, or persecute, or commit other human rights abuses. For example, a group of Israeli intelligence veterans have accused Israel of gathering information about Palestinians' sexual orientation and other private matters for "political persecution" and to "create divisions in Palestinian society."[194] The NSA's transfer of intelligence data under the MOU reportedly contains the e-mails and phone calls of many Arab- or Palestinian-Americans, whose friends and relatives could become targets based on these communications.[195]

DISSEMINATION TO FOREIGN GOVERNMENTS OF FOREIGN-TO-FOREIGN COMMUNICATIONS ACQUIRED UNDER FISA

Although FISA procedures prohibit the NSA from sharing "domestic communications and communications to and from United States persons" with foreign governments, it is possible that the NSA's foreign counterparts have access to some of these communications through joint intelligence gathering operations.[196] The procedures also permit the sharing of foreign-to-foreign communications that refer to or are otherwise about U.S. persons obtained under FISA, subject to certain restrictions. Such communications may be shared if the U.S.: (1) obtains a "written assurance" from the foreign government that it will follow the retention and dissemination procedures that the Foreign Intelligence Surveillance Court has established for handling such communications; and (2) adheres to certain minimization or auditing requirements, as follows:[197]

- For *unencrypted* foreign-to-foreign communications, the NSA may share them with foreign governments only after it has removed all "references to [U.S.] persons that are not necessary to understand or assess the foreign intelligence" contained in the communication.[198] The definition of "foreign intelligence" under FISA is not as broad as EO 12333's, but it still encompasses any information concerning U.S. persons that is "necessary to" the conduct of foreign affairs or the country's security.[199]

- For *encrypted* foreign-to-foreign communications, the NSA need only adhere to post-sharing auditing requirements. The NSA is required to review annually a "representative sampling" of those encrypted communications that have been shared (and later decrypted) to ensure that references to U.S. persons are necessary to understand or assess foreign intelligence.[200] Only upon such a review will the NSA take "corrective measures" to remove any unnecessary references.[201] This after-the-fact audit is inadequate to protect the privacy rights of U.S. persons. If the foreign government manages to decrypt the communications provided to it by the U.S. government, it is likely to have access to troves of innocuous personal and sensitive information about Americans, particularly as encryption becomes more common. It is also unclear what "corrective measures" the NSA takes (or can take) to remedy the resulting privacy violation, and how these measures would address those communications that fall outside the "representative sampling."

V. OVERSIGHT

The intelligence agencies' broad powers are generally not subject to the types of external oversight that could prevent large-scale violations of privacy and abuse of authority, and that is particularly true for surveillance under EO 12333. Intelligence agencies are accountable primarily to themselves when they conduct surveillance under the Order. Legislative oversight is spotty, and judicial oversight non-existent. Given that EO 12333 programs capture a large volume of U.S. persons' communications, this lack of external oversight leaves Americans' constitutionally protected privacy, speech, and association rights vulnerable.

A. Congressional Oversight

While Congress has the authority to oversee EO 12333 surveillance, such oversight has been minimal in practice.[202] The National Security Act requires intelligence agencies to keep the congressional intelligence committees "fully and currently informed of all intelligence activities," but the duty to inform is limited as follows.[203]

The National Security Act provides the President with the discretion to withhold information about "covert actions" from all of Congress except a select group of congressional leaders known as the "Gang of Eight," if he or she determines that such withholding is essential to protect vital U.S. interests.[204] The Act defines "covert action" as any activity the government secretly takes to "influence political, economic, or military conditions abroad," but states that this does not include "activities the *primary* purpose of which is to acquire intelligence."[205] It is unclear under what circumstances an operation that serves both "covert" and surveillance functions (for example, an operation that seeks to both destabilize a foreign defense communications network and gather communications passing through that network for intelligence analysis) would qualify for "Gang of Eight" notification.

Moreover, the executive branch has traditionally restricted notification of intelligence programs it views as particularly sensitive even further, to the chairs and ranking members of both intelligence committees (commonly known as the "Gang of Four"). Although such a procedure is not authorized by statute, it is a longstanding practice that appears to be "generally accepted by the leadership of the intelligence committees."[206] Critics of such restricted notification argue that it is not only illegal, but also a barrier to effective oversight, as Members that receive such briefings may not "take notes, seek the advice of their counsel, or even discuss the issues raised with their committee colleagues."[207]

There is evidence to suggest that not even the "Gang of Eight" or the "Gang of Four" is notified about certain EO 12333 surveillance activities — possibly because the executive branch is relying on language in the National Security Act that effectively waives notification in cases of "sensitive intelligence sources and methods or other exceptionally sensitive matters."[208] In October 2013, Senator Dianne Feinstein, the former chair and current ranking member of the Senate Select Committee on Intelligence, suggested that the Committee had not been "satisfactorily informed" of intelligence surveillance activities, and that a "total review of all intelligence programs" was necessary.[209] In 2014, the Committee, while still under Senator Feinstein's leadership, initiated an "in-depth review" of intelligence surveillance activities including EO 12333 programs. This review sought to "identify, describe, and assess" the "governance,

cost-effectiveness, legal authorities, and cross-[agency] integration" of these activities.[210] However, following a change in committee leadership in 2015, it is unclear whether this review is still ongoing.

Arguably, the sheer scale of the intelligence establishment today has outstripped the capacity of the 22-member House Permanent Select Committee on Intelligence and the 15-member Senate Select Committee on Intelligence (along with their staffers) to perform effective oversight. Today's Intelligence Community consists of seventeen agencies and hundreds of thousands of employees, with a declared budget of almost 70 billion dollars.[211] These agencies conduct surveillance operations that gather millions of electronic communications and other pieces of data on a daily basis, and they are sure to exploit future advances in technology to expand intelligence gathering opportunities. The rapid growth of the intelligence enterprise "challenges the capacity of existing oversight and accountability structures, particularly where private contractors and other non-government entities are involved."[212]

B. Internal Oversight

The government claims that internal oversight mechanisms are "extensive and multi-layered," but the secrecy of intelligence operations makes it difficult to assess claims about the effectiveness of such oversight mechanisms.[213] The Privacy and Civil Liberties Oversight Board is conducting in-depth examinations of NSA and CIA programs under EO 12333, but has noted that its review is limited to counterterrorism activities, and that its findings will be "largely or entirely classified."[214] The public is also unable to scrutinize the methodology and results of audits and investigations conducted by agencies' own oversight personnel, as these generally are classified as well.

More important, purely internal checks and balances can go only so far in protecting privacy and preventing government abuse. To be sure, the intelligence agencies' oversight offices are critical tools of accountability. However, as former senior Department of Homeland Security (DHS) official and intelligence law expert Margo Schlanger explains, such internal oversight has become infused with a culture of "legalism," which treats legal restrictions and procedures "as a ceiling rather than a floor."[215] This preoccupation with technical legal compliance leaves "little room … for [the] more conceptual weighing of interests and options" that is necessary to achieve surveillance policies that optimally balance security and liberty.[216] Moreover, institutional allegiance leads the overseers to interpret the law in a manner that is more permissive than an objective reading might allow.[217]

Furthermore, many internal oversight offices have specific limitations. For example, Professor Shirin Sinnar's examination of Inspector Generals' offices shows that they do not typically evaluate violations of constitutional rights, have little or no capacity to obtain relief for individual victims of rights violations, and typically lack power to enforce their recommendations.[218]

C. Judicial Oversight

The courts have traditionally been an important external safeguard to help ensure that government surveillance activities remain accountable to constitutional values and the rule of law. Yet the courts play no role in overseeing EO 12333 activities.

While the executive branch has long considered EO 12333 surveillance to be an exercise of the President's powers as commander-in-chief, this power "does not remove constitutional limitations safeguarding essential liberties."[219] The sheer quantity and quality of U.S. persons' communications implicated by EO 12333 surveillance in the digital age raises significant First and Fourth Amendment concerns. As the primary institutions of rights enforcement, courts are a critical bulwark against executive overreach, especially in the "often competitive" realm of intelligence gathering.[220] The independence of judges also facilitates "neutral and detached" judgment about the proper scope of surveillance activities in light of the security and liberty interests at stake.[221]

Establishing judicial oversight of intelligence surveillance overseas may not necessarily require adherence to the traditional warrant process. But as transnational surveillance of digital communications becomes increasingly pervasive, the need for independent, external oversight becomes more pressing.

VI. OPEN QUESTIONS

As this report shows, intelligence agencies have wide-ranging powers to gather, store, analyze, and share communications and data about Americans and citizens of other countries. Publicly available regulations suggest that there are few robust constraints on these powers. However, key aspects of how these authorities are exercised and regulated remain secret. In the last few months, the Director of National Intelligence has taken important steps in declassifying and releasing information that helps policymakers and the American people understand how the NSA's operations work. But much remains hidden, as set out in the list of "known unknowns" below.

A. Secret Laws

While many of the agencies' internal procedures are publicly available, it is unclear how they are interpreted and applied. It is also unclear whether the publicly available regulations — some of which were established more than three decades ago — have been amended, and how they are applied to new surveillance technologies and programs. Moreover, some agencies' regulations remain classified. The public deserves to know how the agencies interpret their duties and obligations under the Constitution and international law.

1. **Legal interpretations:** How do relevant federal agencies (including the Justice Department's Office of Legal Counsel, the NSA, CIA, and ODNI) and the White House interpret the legality (whether under domestic or international law) and constitutionality of surveillance activities conducted under EO 12333?[222]

2. **Unknown laws:** Are there any other laws, orders and policies besides those disclosed to the public that regulate foreign intelligence surveillance overseas?

B. Oversight

The public cannot simply rely on the government's word that intelligence oversight is robust. To back up this claim, the government should explain in detail how Congress and the agencies themselves ensure independent and effective oversight under EO 12333.

3. **Congress:** What does the congressional oversight regime for EO 12333 look like? How frequently does the executive branch brief the intelligence committees, other groups of members, and Congress as a whole on EO 12333 surveillance? What kinds of information are provided to Congress about such activities, and what is withheld?

4. **Funding:** How does Congress allocate funds for surveillance activities and programs conducted under EO 12333? Have these activities and programs been audited?

5. **Outsourcing:** What kinds of intelligence activities conducted under EO 12333 are outsourced to private contractors? What rules and regulations are in place to ensure that these contractors respect privacy, civil liberties, and relevant U.S. and international laws when they conduct such activities?

6. **Internal Oversight:** How frequently is compliance with internal procedures under EO 12333, PPD-28, and all other relevant laws and policies reviewed internally? What is the nature and frequency of reported incidents of non-compliance, and what recommendations have the relevant oversight bodies made to prevent future incidents and to ensure respect for privacy and civil liberties? How faithfully have these recommendations been implemented?

7. **Effectiveness:** How is the effectiveness of intelligence activities conducted under EO 12333 assessed, which government entities conduct these assessments, and how frequently do such assessments occur?

C. Information Gathering

Our analysis raises fundamental questions about how the NSA gathers information overseas, and the kinds of restrictions that EO 12333, PPD-28, and their subsidiary regulations impose on such information gathering.

8. **Gathering vs. collection:** Is the term "collection" interpreted differently from the terms "interception," "gathering," and "acquisition"? What are some examples to help illustrate the government's definitions of "collection" under the subsidiary regulations? If "collection" means something other than "gathering," are there any rules regulating information gathering under EO 12333?

9. **Impact of EO 12333 surveillance on U.S. persons:** To what extent do electronic surveillance activities conducted under EO 12333 gather: (1) communications between U.S. persons and non-U.S. persons; and (2) wholly domestic communications between U.S. persons?

10. **Bulk vs. targeted surveillance:** How much of EO 12333 surveillance involves "bulk" (versus "targeted") information gathering? Under what circumstances does the government resort to "bulk" information gathering?

11. **Search terms:** What kinds of search terms are used to obtain or process information under EO 12333 (e.g., personal identifiers such as names or e-mail accounts; less specific identifiers such as IP addresses; geographic areas; indicia of encryption; substantive topics; etc.)? Which are most commonly used, and how much information does each type of search term collect?

12. **Joint information gathering with foreign governments:** What rules and regulations apply to intelligence gathering activities that are conducted jointly with foreign governments?

D. Use, Retention, and Sharing of Information

Our analysis also prompts questions about how information gathered under EO 12333 is processed, used, stored, retained and shared.

13. **Procedures governing inter-agency sharing:** Which agencies other than the collecting agency have access to EO 12333 data (processed or unprocessed)? How is such access regulated, and what is the process by which decisions to mask or delete data before sharing are made?

14. **Use in criminal, immigration, and other proceedings:** Are there any criminal cases or immigration proceedings where the government has relied on evidence (a) directly obtained or (b) derived from EO 12333 surveillance? Are there any other legal or administrative proceedings where the government has relied on evidence directly obtained or derived from EO 12333 surveillance? How many of these cases exist, and how many or what proportion of them resulted in adverse action (e.g., conviction or deportation)?

15. **Notification of criminal defendants and other parties:** Under what circumstances, if at all, are criminal defendants and other parties to legal proceedings notified when information obtained or derived through EO 12333 activities is used against them?

16. **Information sharing with foreign governments:** Are there requirements in addition to or more specific than those in publicly available directives for determining how and what data is shared with foreign governments? How are the equities weighed when sharing intelligence with governments that have a history of committing human rights abuses? What safeguards are included in information sharing agreements with foreign governments to ensure that the privacy and human rights of both American and foreign citizens are protected? What are the obligations of the government in cases where it determines that shared information is being used to conduct human rights abuses?

CONCLUSION

The extent of the National Security Agency's overseas operations and how these operations are regulated are in many respects a black box. While there are no doubt operational details that must remain secret, the Agency should share with Congress and the American people information necessary to understand the scope of its programs and the legal parameters within which they operate. The need for transparency is particularly urgent given that EO 12333 operations constitute the largest and — as our analysis suggests — potentially most intrusive of the nation's surveillance activities. The fact that they are conducted abroad rather than at home makes little difference in an age where data and information flows are unconstrained by geography, and where the constitutional rights of Americans are just as easily compromised by operations in London as those in Los Angeles.

ANNEX: THE SCOPE OF FISA

When FISA was enacted, it applied only to specific categories of "electronic surveillance," which excluded some NSA acquisition of electronic communications on U.S. soil, as well as NSA electronic acquisition that targeted U.S. persons overseas. 50 U.S.C. §1801(f). In 2008, FISA was amended to cover all electronic surveillance activities that target U.S. persons, regardless of the location of the target or where the information was gathered. FISA reserves the most restrictive procedures for this type of surveillance, generally prohibiting the government from targeting a U.S. person unless it obtains a FISA court order establishing probable cause that the target is a foreign power or an agent of a foreign power.

FISA's applicability is more complex when foreign intelligence surveillance is conducted in a way that does not target a U.S. person. The table below provides a comprehensive breakdown of the scope of FISA's coverage when the NSA conducts foreign intelligence surveillance that does not target U.S. persons:

IF SURVEILLANCE DOES NOT TARGET U.S. PERSONS…			
i.e., if surveillance is not targeted, if it targets non-U.S. persons or "persons reasonably believed to be located abroad," or if it uses information gathering techniques not based on communicants' identity (e.g., content-based search terms, or selection of enciphered communications) …			
What type of communication was acquired?	**Where was the communication acquired?**	**Where are communicants located?**	**Does FISA apply?**
Wire	U.S.	U.S.	Yes
	U.S.	One end U.S., one end overseas	Yes
	U.S.	Overseas	No
	Overseas	U.S.	No
	Overseas	One end U.S., one end overseas	No
	Overseas	Overseas	No
Radio	U.S.	U.S.	Yes
	U.S.	One end U.S., one end overseas	No
	U.S.	Overseas	No
	Overseas	U.S.	Yes
	Overseas	One end U.S., one end overseas	No
	Overseas	Overseas	No
Stored	U.S.	U.S.	Yes
	U.S.	One end U.S., one end overseas	Yes
	U.S.	Overseas	Yes
	Overseas	U.S.	No
	Overseas	One end U.S., one end overseas	No
	Overseas	Overseas	No

ENDNOTES

1 Declassified Presentation, Office of Gen. Counsel, Nat'l Sec. Agency, Slide 83, *available at* http://www.dni.gov/files/documents/1118/CLEANED021.extracts.%20Minimization%20Pr...cted%20from%20file%20021-Sealed.pdf.

2 In particular, reform efforts have largely focused on Section 215 of the PATRIOT Act, which the Agency used to create a vast database of information about Americans' telephone calls. *See* Glenn Greenwald, *NSA Collecting Phone Records of Millions of Verizon Customers Daily,* Guardian (June 6, 2013), http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order. On June 2, 2015, Congress enacted the USA FREEDOM Act, which, *inter alia*, prohibited "bulk collection" and imposed additional targeting and oversight requirements for the government to obtain telephone call records. USA FREEDOM Act of 2015, Pub. L. No. 114-23, 129 Stat. 268 (2015).

3 Exec. Order No. 12,333, 3 C.F.R. 200 (1981).

4 *Id.* at § 2.3. Section 2.3 stipulates ten categories of information that intelligence agencies may "collect, retain or disseminate:" (a) Information that is publicly available or collected with the consent of the person concerned; (b) Information constituting foreign intelligence or counterintelligence, including such information concerning corporations or other commercial organizations; (c) information obtained in the course of a lawful foreign intelligence, counterintelligence, international narcotics or international terrorism investigation; (d) Information needed to protect the safety of any persons or organizations, including those who are targets, victims or hostages of international terrorist organizations; (e) Information needed to protect foreign intelligence or counterintelligence sources or methods from unauthorized disclosure; (f) Information concerning persons who are reasonably believed to be potential sources or contacts for the purpose of determining their suitability or credibility; (g) Information arising out of a lawful personnel, physical or communications security investigation; (h) Information acquired by overhead reconnaissance not directed at specific United States persons; (i) Incidentally obtained information that may indicate involvement in activities that may violate federal, state, local or foreign laws; and (j) Information necessary for administrative purposes. *Id.*

5 *Id.* at § 3.4(d).

6 Executive orders are written proclamations that "are generally directed to, and govern actions by, Government officials and agencies." Executive orders have the force and effect of law if they stem from "implied constitutional and statutory authority." "In the constitutional context, presidential power is derived from Article II of the U.S. Constitution, which states that 'the executive power shall be vested in a President of the United States,' that 'the President shall be Commander in Chief of the Army and Navy of the United States,' and that the President 'shall take Care that the Laws be faithfully executed.'" Vivian S. Chu & Todd Garvey, Cong. Research Serv., RS20846, Executive Orders: Issuance, Modification, and Revocation 1-2 (2014), *available at* http://fas.org/sgp/crs/misc/RS20846.pdf.

7 Exec. Order No. 12,333 § 2.2, 3 C.F.R. 200 (1981).

8 *Id.* at § 2.

9 *Id.* at § 2.4.

10 *Id.* at § 2.2.

11 *Id.* at § 2.11.

12 *Id.* at § 2.10.

13 *Id.* at § 3.4(h).

14 *See infra* text accompanying notes 69-71.

15 50 U.S.C. § 1801(f).

16 Note that the NSA has not officially acknowledged many of these operations.

17 Morgan Marquis-Boire, Glenn Greenwald & Micah Lee, *XKEYSCORE: NSA's Google for the World's Private Communications*, Intercept (July 1, 2015, 10:49 AM), https://firstlook.org/theintercept/2015/07/01/nsas-google-worlds-private-communications/.

18 For an in-depth pre-Snowden history of the NSA and its activities, see James Bamford's trilogy of books on the subject: James Bamford, The Puzzle Palace: Inside the National Security Agency, America's Most Secret Organization (1st ed. 1983); James Bamford, Body of Secrets: Anatomy of the Ultra-Secret National Security Agency (reprt. ed. 2002); James Bamford, The Shadow Factory: The NSA from 9/11 to the Eavesdropping on America (2009).

19 For instance, the Agency and its foreign partners for decades relied on the program codenamed ECHELON to obtain international communications from satellite transmissions. Duncan Campbell, *They've Got It Taped*, New Statesman Society (Aug. 12, 1988), http://www.duncancampbell.org/menu/journalism/newstatesman/newstatesman-1988/They%27ve%20got%20it%20taped.pdf; Duncan Campbell, *GCHQ and Me: My Life Unmasking British Eavesdroppers,* Intercept (Aug. 3, 2015), https://theintercept.com/2015/08/03/life-unmasking-british-eavesdroppers/. More recently, there is evidence that the NSA relies on EO 12333, as well as the FISA Amendments Act, to replicate much of the function of a discontinued program to collect Americans' internet metadata in bulk. *See, e.g.,* Charlie Savage, Power Wars: Inside Obama's Post-9/11 Presidency 565-66 (2015); Charlie Savage, *File Says N.S.A. Found Way to Replace E-Mail Program*, N.Y. Times (Nov. 19, 2015), *available at* http://www.nytimes.com/2015/11/20/us/politics/records-show-email-analysis-continued-after-nsa-program-ended.html.

20 For instance, the NSA targets Afghanistan via a program codenamed SHIFTINGSHADOW, which obtains voice calls and metadata from the networks of foreign telecommunications providers serving Afghanistan. Peter Koop, *Slides about NSA's Upstream Collection*, electrospaces.net (Jan. 17, 2014), http://electrospaces.blogspot.com/2014/01/slides-about-nsas-upstream-collection.html.

21 Ryan Devereaux, Glenn Greenwald & Laura Poitras, *Data Pirates of the Caribbean: The NSA Is Recording Every Cell Phone Call in the Bahamas*, Intercept (May 19, 2014, 12:37 PM), https://theintercept.com/2014/05/19/data-pirates-caribbean-nsa-recording-every-cell-phone-call-bahamas/. Note that *The Intercept* did not name Afghanistan in its report on MYSTIC because of "specific, credible concerns that doing so could lead to increased violence." The NSA's targeting of Afghanistan was subsequently revealed by Wikileaks. *WikiLeaks statement on the mass recording of Afghan telephone calls by the NSA*, WikiLeaks (May 23, 2014, 5:00 AM), https://wikileaks.org/WikiLeaks-statement-on-the-mass.html.

22 SOMALGET is a part of the MYSTIC program. An NSA document indicates that SOMALGET "processes 'over 100 million call events per day.'" Devereaux, Greenwald & Poitras, *supra* note 21; *see also* Barton Gellman & Ashkan Soltani, *NSA Surveillance Program Reaches 'Into the Past' to Retrieve, Replay Phone Calls*, Wash. Post (Mar. 18, 2014), http://www.washingtonpost.com/world/national-security/nsa-surveillance-program-reaches-into-the-past-to-retrieve-replay-phone-calls/2014/03/18/226d2646-ade9-11e3-a49e-76adc9210f19_story.html. Analysts rely on the audio content to verify their analyses of the metadata. Memorandum from Unidentified Official, International Crime & Narcotics Division S2F, National Security Agency (2012), *available at* https://www.documentcloud.org/documents/1164088-somalget.html.

23 Gellman & Soltani, *NSA Surveillance Program Reaches, supra* note 22.

24 Barton Gellman & Ashkan Soltani, *NSA Infiltrates Links to Yahoo, Google Data Centers Worldwide, Snowden Documents Say*, Wash. Post (Oct. 30, 2013) [hereinafter Gellman & Soltani, *NSA Infiltrates Links*], http://www.washingtonpost.

com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html; *see also* Barton Gellman & Ashkan Soltani, *NSA Collects Millions of E-Mail Address Books Globally*, Wash. Post, (Oct. 14, 2013), http://www.washingtonpost.com/world/national-security/nsa-collects-millions-of-e-mail-address-books-globally/2013/10/14/8e58b5be-34f9-11e3-80c6-7e6dd8d22d8f_story.html.

25 Gellman & Soltani, *NSA Infiltrates Links*, *supra* note 24.

26 *Id.*

27 David E. Sanger & Nicole Perlroth, *Internet Giants Erect Barriers to Spy Agencies*, N.Y. Times (June 6, 2014), *available at* http://www.nytimes.com/2014/06/07/technology/internet-giants-erect-barriers-to-spy-agencies.html.

28 These programs appear to be part of a suite of programs collectively codenamed OAKSTAR. MONKEYROCKET is focused on counterterrorism in the Middle East, Europe and Asia, while MADCAPOCELOT is focused on counterterrorism in Europe and Russia. Koop, *Slides About NSA's Upstream Collection*, *supra* note 20.

29 *Id.*

30 Spencer Ackerman & James Ball, *Optic Nerve: Millions of Yahoo Webcam Images Intercepted by GCHQ*, Guardian (Feb. 28, 2014, 5:31 AM), http://www.theguardian.com/world/2014/feb/27/gchq-nsa-webcam-images-internet-yahoo. Relatedly, the NSA also obtains faces from millions of web images for use in its facial recognition programs. James Risen and Laura Poitras, *N.S.A. Collecting Millions of Faces from Web Images*, N.Y. Times (May 31, 2014), http://www.nytimes.com/2014/06/01/us/nsa-collecting-millions-of-faces-from-web-images.html.

31 James Ball, *NSA Collects Millions of Text Messages Daily in 'Untargeted' Global Sweep*, Guardian (Jan. 16, 2014), http://www.theguardian.com/world/2014/jan/16/nsa-collects-millions-text-messages-daily-untargeted-global-sweep. According to *The Guardian*, communications from U.S. phone numbers may have been removed from the database, but those of other countries, including the U.K., were retained. *Id.*

32 *Id.*

33 Classified Slide Show from the National Security Agency, Slide 7 (June 9, 2011), *available at* http://www.theguardian.com/world/interactive/2014/jan/16/nsa-dishfire-text-messages-documents. It is unclear whether the GCHQ employs PREFER as well.

34 Jeff Larson, James Glanz & Andrew W. Lehren, *Spy Agencies Probe Angry Birds and Other Apps for Personal Data*, ProPublica (Jan. 27, 2014) https://www.propublica.org/article/spy-agencies-probe-angry-birds-and-other-apps-for-personal-data.

35 *Id.*

36 Julia Angwin and Jeff Larson, *FAQ About NSA's Interest in Angry Birds and Other 'Leaky Apps*,' ProPublica (Jan. 28, 2014), https://www.propublica.org/article/faq-about-nsas-interest-in-angry-birds-and-other-leaky-apps.

37 Larson et al., *supra* note 34.

38 *Id.*

39 The database is codenamed "FASCIA." Barton Gellman & Ashkan Soltani, *NSA Tracking Cellphone Locations Worldwide, Snowden Documents Show,* Wash. Post (Dec. 4, 2013), http://www.washingtonpost.com/world/national-security/nsa-tracking-cellphone-locations-worldwide-snowden-documents-show/2013/12/04/5492873a-5cf2-11e3-

bc56-c6ca94801fac_story.html. Note, however, that the NSA denies that it is "intentionally collecting bulk cellphone location information about cellphones in the United States." *Id.* Nevertheless, *The Washington Post* observes that bulk gathering of cell phone location information outside the U.S. inevitably sweeps in the tens of millions of U.S. mobile phone users who travel abroad every year. *Id.*

40 Under a sub-program codenamed "STORMBREW," the NSA relies on "two unnamed corporate partners" to administer the NSA's interception equipment. STORMBREW acquires data from 27 telephone links that transfer traffic from one provider's internal network to another's. *Id.*

41 *Id.*

42 *Id.*

43 Ryan Gallagher & Peter Maass, *Inside the NSA's Secret Efforts to Hunt and Hack System Administrators*, Intercept (Mar. 20, 2014, 7:07 PM), https://firstlook.org/theintercept/2014/03/20/inside-nsa-secret-efforts-hunt-hack-system-administrators/.

44 *Id.*

45 James Ball, Bruce Schneier & Glenn Greenwald, *NSA and GCHQ Target Tor Network that Protects Anonymity of Web Users*, Guardian (Oct. 4, 2013, 10:50 AM), http://www.theguardian.com/world/2013/oct/04/nsa-gchq-attack-tor-network-encryption; Bruce Schneier, *Attacking Tor: How the NSA Targets Users' Online Anonymity,* Guardian (Oct. 4, 2013, 10:50 AM), http://www.theguardian.com/world/2013/oct/04/tor-attacks-nsa-users-online-anonymity.

46 *Tor Metrics — Direct Users by Country*, https://metrics.torproject.org/userstats-relay-country.html?graph=userstats-relay-country&start=2014-11-22&end=2015-02-20&country=all&events=off (last visited Feb. 25, 2015).

47 Marquis-Boire, Greenwald & Lee, *supra* note 17. There are at least three other NSA databases: "MARINA," which contains "User Activity" metadata; "PINWALE," which contains "content selected from dictionary tasked terms" (i.e. content that is derived from targeted searches) and "TRAFFICTHIEF," which contains metadata gleaned from "a subset of tasked strong-selectors" (i.e. metadata derived from searches that the NSA believes are highly targeted). Glenn Greenwald, *XKEYSCORE: NSA Tool Collects 'Nearly Everything a User Does on the Internet'*, Guardian (July 31, 2013, 8:56 AM), http://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data. The NSA also has a database of financial information codenamed "TRACFIN," but it is unclear which programs gather such data, and whether it is gathered under EO 12333. *'Follow the Money': NSA Spies on International Payments*, Spiegel Online Int'l (September 15, 2013, 10:16 AM), http://www.spiegel.de/international/world/spiegel-exclusive-nsa-spies-on-international-bank-transactions-a-922276.html.

48 Marquis-Boire et al., *supra* note 17.

49 *Id.*

50 For example, training slides show that the justifications offered for searches can be as brief as "ct target in n africa" and "Swedish Extremist website visitors." Greenwald, *XKEYSCORE, supra* note 37.

51 A training slide shows that "foreignness factors" — which demonstrate that a search does not target a U.S. person — can be selected from a dropdown menu. *Id.*

52 While the auditing requirements for queries of EO 12333 surveillance data are not publicly available, those for queries of data obtained under Section 702 of the Foreign Intelligence Surveillance Act might shed some light. The NSA "maintains audit trails for all queries of the Section 702 data," and the "NSA's Signals Intelligence Directorate's compliance staff routinely reviews a portion of all queries that include U.S. person identifiers to ensure that all such queries are only conducted when appropriate." NSA Director of Civil Liberties and Privacy Office, NSA's Implementation of

Foreign Intelligence Surveillance Act section 702 7 (Apr. 16, 2014), *available at* https://www.nsa.gov/civil_liberties/_files/nsa_report_on_section_702_program.pdf. Snowden has mentioned, however, that the "majority of the people who are doing the auditing are the friends of the analysts. They work in the same office. They're not full-time auditors, they're guys who have other duties assigned. There are a few traveling auditors who go around and look at the things that are out there, but really it's not robust." Marquis-Boire, Greenwald & Lee, *supra* note 17.

53 Marquis-Boire, Greenwald & Lee, *supra* note 17; *'Prolific Partner': German Intelligence Used NSA Spy Program*, Spiegel Online Int'l (July 20, 2013, 6:02 PM), http://www.spiegel.de/international/germany/german-intelligence-agencies-used-nsa-spying-program-a-912173.html.

54 Glenn Greenwald, Laura Poitras & Ewan MacAskill, *NSA Shares Raw Intelligence Including Americans' Data with Israel*, Guardian (Sept. 11, 2013, 10:40 AM), http://www.theguardian.com/world/2013/sep/11/nsa-americans-personal-data-israel-documents.

55 Among some of the data that the NSA has successfully decrypted are Facebook chats, Skype calls, visits to "https" websites (the "s" stands for secure), and Virtual Private Network (VPN) connections. SPIEGEL Staff, Pr*ying Eyes: Inside the NSA's War on Internet Security, Spiegel Online Int*'l (Dec. 28, 2014, 8:01 PM), http://www.spiegel.de/international/germany/inside-the-nsa-s-war-on-internet-security-a-1010361.html.

56 For example, the NSA has, with the help of Microsoft, obtained pre-encryption access to e-mails and web chats on Outlook.com. Glenn Greenwald et al., Mi*crosoft Handed the NSA Access to Encrypted Messages,* Guardian (July 12, 2013, 3:04 AM), http://www.theguardian.com/world/2013/jul/11/microsoft-nsa-collaboration-user-data.

57 Classified Document, Nat'l Sec. Agency, Computer Network Operations: SIGINT Enabling Project, *available at* http://www.propublica.org/documents/item/784280-sigint-enabling-project.

58 Larry Greenemeier, NSA Effor*ts to Evade Encryption Technology Damaged U.S. Cryptography Standard,* Sci. Am. (Sept. 18, 2013), http://www.scientificamerican.com/article/nsa-nist-encryption-scandal/.

59 Nicole Perlroth, S*ecurity Experts Oppose Government Access to Encrypted Communication,* N.Y. Times (July 7, 2015), http://www.nytimes.com/2015/07/08/technology/code-specialists-oppose-us-and-british-government-access-to-encrypted-communication.html; *Conor Friedersdorf, Former National-Security Officials Now See the Peril of Weakening Encryption,* The Atlantic (July 30, 2015), http://www.theatlantic.com/politics/archive/2015/07/former-national-security-officials-see-the-peril-of-weakening-encryption/399848/.

60 Harold Abelson, et al., Keys Under Doormats: Mandating Insecurity By Requiring Government Access to All Data and Communications 24-25 (July 6, 2015), https://dspace.mit.edu/bitstream/handle/1721.1/97690/MIT-CSAIL-TR-2015-026.pdf.

61 John Napier Tye, *Meet Executive Order 12333: The Reagan Rule That Lets the NSA Spy on Americans*, Wash. Post (July 18, 2014), http://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.

62 In 2013, analysts estimated that "by the end of 2013, there will be some 600 million personal cloud storage subscriptions, and that number is expected to double by the end of 2017." Deloitte, The State of The Global Mobile Consumer, 2013 Divergence Deepens (2013), http://www2.deloitte.com/content/dam/Deloitte/global/Documents/Technology-Media-Telecommunications/dttl_TMT-GMCS_January%202014.pdf.

63 *See generally* Jeffrey Hoffer, et al., Modern Database Management 13-1, 13-4 to -5 (12th ed. 2015). Multiple copies help prevent permanent loss of data and ensure that the data is easily accessible even if the user switches location or if a particular data center experiences a power outage or undergoes maintenance.

64 For example, the New York Times website uses (among other third-party services) Google's Doubleclick service, which

provides the ads for the site. When a user visits www.nytimes.com, the user's browser will connect not only to the Times' server, but also to the Doubleclick server and the servers of all the other third parties included by the site. *Privacy Policy,* N.Y. Times (June 10, 2015), http://www.nytimes.com/content/help/rights/privacy/policy/privacy-policy.html.

65 Steven Englehardt et al., Cookies That Give You Away: The Surveillance Implications of Web Tracking, § 5.2 (2015), http://www.cs.princeton.edu/~ste/papers/www15_cookie_surveil.pdf.

66 The scope of Congress's authority to regulate overseas surveillance is the subject of some debate. It is widely acknowledged that the president has authority to conduct at least some kinds of overseas surveillance under Article II of the Constitution — an authority rooted in the president's commander-in-chief function and the executive branch's primacy in foreign affairs and national security. *See* Transcript of Privacy and Civil Liberties Oversight Board Public Meeting, Public Meeting on Executive Order 12333 at 27-30 (May 13, 2015), *available at* https://www.pclob.gov/library/20150513-Transcript.pdf (statement of Robert Chesney, Charles I. Francis Prof. in Law and Assoc. Dean for Academic Affairs, University of Texas Sch. of Law) (discussing some of the factors that determine whether Congress has power to regulate surveillance). However, several constitutional law experts have observed that this authority is not exclusive, and that the Constitution also gives Congress important oversight and regulatory powers in the areas of war making, foreign relations, and national defense. *See* Transcript of Privacy and Civil Liberties Oversight Board Public Meeting, Public Meeting on Executive Order 12333 at 31-38 (May 13, 2015), *available at* https://www.pclob.gov/library/20150513-Transcript.pdf (statement of Deborah Pearlstein, Ass't Prof. of Law, Benjamin N. Cardozo Sch. of Law). A full explanation of this debate is beyond the scope of this paper. However, particularly given this report's conclusion that EO 12333 surveillance sweeps in large numbers of Americans' communications (including wholly domestic ones), we proceed on the assumption that the President is bound by law when conducting this type of surveillance. Indeed, EO 12333 itself appears to embrace this assumption, as it includes a rule of construction that "Nothing in this Order shall be construed to authorize any activity in violation of the Constitution or statutes of the United States." Exec. Order No. 12,333 § 2.8, 3 C.F.R. 200 (1981).

67 Exec. Order No. 12,333 § 2.3, 3 C.F.R. 200 (1981).

68 *Id.*

69 Office of the Dir. of Nat'l Intelligence, Status of Attorney General Approved U.S. Person Procedures Under E.O. 12333 (Feb. 10, 2015), https://www.pclob.gov/library/EO12333-AG-Guidelines-February-10-2015.pdf.

70 *Id.* The DHS's and USCG's interim procedures are public. *See* Memorandum Re: Interim Intelligence Oversight Procedures for the Office of Intelligence & Analysis from Charles E. Allen, Undersec'y for Intelligence and Analysis, Dep't of Homeland Sec., and Matthew L. Kronish, Assoc. Gen. Counsel (Intelligence) to All Employees, Detailees, and Contractors Supporting the Office of Intelligence and Analysis (Apr. 3, 2008), *available at* http://www.dhs.gov/sites/default/files/publications/interim-intelligence-oversight-procedures-%20for-the-office-of-intelligence-and-analysis.pdf; U.S. Coast Guard, Coast Guard Intelligence Activities, COMDTINST M3820.12 (Aug. 28, 2003) [hereinafter Coast Guard Intelligence Activities], *available at* http://www.uscg.mil/directives/cim/3000-3999/CIM_3820_12.pdf. The DEA operates under AG-approved "Guidelines for Disclosure of Grand Jury and Electronic, Wire, and Oral Interception Information Identifying United States Persons." Memorandum Re: Guidelines for Disclosure of Grand Jury and Electronic, Wire, and Oral Interception Information Identifying United States Persons, from John Ashcroft, Att'y Gen., to Heads of Dep't Components (Sept. 23, 2002), *available at* http://www.dni.gov/index.php/about/organization/ic-legal-reference-book-2012/ref-book-disclosure-of-information-identifying-usps. The DEA is also subject to the "Guidelines Regarding Disclosure to the Director of Central Intelligence and Homeland Security Officials of Foreign Intelligence Acquired in the Course of a Criminal Investigation," *See* Memorandum Re: Guidelines Regarding Disclosure to the Director of Central Intelligence and Homeland Security Officials of Foreign Intelligence Acquired in the course of a Criminal Investigation, from John Ashcroft, Att'y Gen., to Heads of Dep't of Justice Components and Heads of Fed. Dep'ts and Agencies with Law Enforcement Responsibilities (Sept. 23, 2002), *available at* http://www.dni.gov/index.php/about/organization/ic-legal-reference-book-2012/ref-book-foreign-intelligence-acquired-in-the-course-of-a-criminal-investigation. The Department of Treasury relies solely on the guidance of in-house counsel.

71 Office of the Dir. of Nat'l Intelligence, *supra* note 69, at 1, 3.

72 Dep't of Defense, Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons, DoD 5240 1-r (Dec. 1982) [hereinafter DoD USP Procedures], *available at* http://www.dtic.mil/whs/directives/corres/pdf/524001r.pdf.

73 Nat'l Sec. Agency, Legal Compliance and U.S. Persons Minimization Procedures, USSID SP0018 (Jan. 25, 2011) [hereinafter USSID 18], *available at* http://www.dni.gov/files/documents/1118/CLEANEDFinal%20USSID%20SP0018.pdf.

74 There is a subtle difference between FISA and EO 12333 in this regard: FISA considers "an alien lawfully admitted for permanent residence" to be a U.S. person, 50 U.S.C. § 1801(i), whereas EO 12333 would only consider "an alien known by the intelligence element concerned to be a permanent resident alien" to be a U.S. person, Exec. Order 12,333 § 3.4(i), 3 C.F.R. 200 (1981). Under EO 12333, it appears that the NSA could treat a permanent resident target as a non-U.S. person as long as it does not know his or her immigration status. For surveillance conducted under FISA, however, that target would be entitled to all the protections afforded to U.S. persons, regardless of the NSA's knowledge.

75 50 U.S.C. § 1801(i); Exec. Order 12,333 § 3.4(i), 3 C.F.R. 200 (1981).

76 Barton Gellman et al., *In NSA-Intercepted Data, Those Not Targeted Far Outnumber the Foreigners Who Are,* Wash. Post (July 5, 2014), https://www.washingtonpost.com/world/national-security/in-nsa-intercepted-data-those-not-targeted-far-outnumber-the-foreigners-who-are/2014/07/05/8139adf8-045a-11e4-8572-4b1b969b6322_story.html.

77 Dep't of Defense, DoD 5240.1R Intelligence Activities (Sept. 22, 2014), *available at* https://www.aclu.org/files/assets/eo12333/DIA/Intelligence%20Activities%20Legal%20Summary%20Card,%20DoD%205240.IR%20Intelligence%20Activities.pdf.

78 Note that a DOJ review found that the rate at which the NSA's targeting decisions resulted in the selection of U.S. persons' communications or communications of someone in the U.S. was 0.4%. Privacy and Civil Liberties Oversight Board, Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act 118 (July 2, 2014), *available at* https://www.nsa.gov/civil_liberties/_files/pclob_section_702_report.pdf. However, this percentage is based only on a review of one year of data, is limited to data gathered under Section 702 of FISA and not EO 12333, which is the subject of this paper, and catches only discovered errors. Furthermore, given the quantity of electronic communications and data that the NSA is gathering, even a small percentage is likely to yield large amounts of U.S. persons' information.

79 Exec. Office of the president, Presidential Policy Directive/PPD-28 (2014) [hereinafter PPD-28], *available at* https://www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities. As a presidential directive, PPD-28 has the same legal effect as an executive order. The Department of Justice has stated that both are presidential orders that are legally binding on the relevant executive agencies; they do not "automatically lapse upon a change of administration," and generally "remain effective until subsequent presidential action is taken." Legal Effectiveness of a Presidential Directive, As Compared to an Executive Order, 24 Op. O.L.C. 29 (2000).

80 PPD-28, *supra* note 79, at § 4.

81 Nat'l Sec. Agency, PPD-28 Section 4 Procedures (Jan. 12, 2015) [hereinafter NSA PPD-28 Procedures], *available at* https://www.nsa.gov/public_info/_files/nsacss_policies/PPD-28.pdf. Note that the DoD has adopted the NSA's PPD-28 procedures as their own. Memorandum from Michael G. Vickers, Under Sec'y of Defense to Director of Nat'l Intelligence (Jan. 20, 2015), *available at* http://fas.org/irp/doddir/dod/dod-ppd-28.pdf.

82 Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, 92 Stat. 1783 (codified in scattered sections of 8, 18, 47, 50 U.S.C.).

83 This would include both operations that originate in the U.S. but target U.S. persons overseas, as well as operations that originate overseas and target U.S. persons. 50 U.S.C. § 1881b. Note that a FISC order is required only when the targeted U.S. person is entitled to a "reasonable expectation of privacy and a warrant would be required if the acquisition were conducted inside the United States for law enforcement purposes." 50 U.S.C. §1881c.

84 USSID 18, *supra* note *73.*

85 Exec. Order 12,333 § 2.8, 3 C.F.R. 200 (1981).

86 50 U.S.C. § 1801(f).

87 Jonathan Mayer, *Executive Order 12333 on American Soil, and Other Tales from the FISA Frontier,* Web Policy (Dec. 3, 2014), http://webpolicy.org/2014/12/03/eo-12333-on-american-soil/. Mayer argues that since such activities are covered neither by FISA nor by any other relevant statute (in particular, the Stored Communications Act) it is likely that the NSA is relying on EO 12333.

88 The U.S. government has argued that foreign targets located overseas have no Fourth Amendment rights (citing *United States v. Verdugo-Urquidez*, 494 U.S. 259 (1990)), and that no additional protections apply to non-targets (including Americans) whose communications are "incidentally" obtained when a foreign target is wiretapped. As detailed in the Brennan Center's report, *What Went Wrong With the FISA Court*, this argument extrapolates beyond what the case law supports. *Verdugo-Urquidez*, with its several opinions, is more properly understood to hold that the Fourth Amendment does not require a warrant when searching the property of foreigners overseas — a much more limited holding. Elizabeth Goitein & Faiza Patel, Brennan Ctr for Justice, What Went Wrong With the FISA Court 12, n.52 (2015), https://www.brennancenter.org/sites/default/files/analysis/What_Went_%20Wrong_With_The_FISA_Court.pdf. As for the case law endorsing "incidental" surveillance, it is comprised of cases in which the government obtained a warrant to wiretap the target, thus affording some vicarious protection to those "incidentally" caught up in the surveillance. *Id.* at 35. For additional analysis of the application of the Fourth Amendment to EO 12333 surveillance, *see* Letter from American Civil Liberties Union to the Privacy and Civil Liberties Oversight Board (Jan. 13, 2016), https://www.aclu.org/letter/aclu-comments-privacy-and-civil-liberties-oversight-board-its-review-executive-order-12333.

89 The government has argued that there is a broad "foreign intelligence exception" to the Fourth Amendment's warrant requirement, and so surveillance for foreign intelligence purposes — even under circumstances where the Fourth Amendment would clearly apply — need only be "reasonable." In reviewing Section 702 of FISA, the Foreign Intelligence Surveillance Court deemed domestic surveillance of communications between U.S. persons and foreign targets to be "reasonable" despite the absence of any individualized judicial finding or any criterion that the target be an agent of a foreign power. We address this holding thoroughly in *What Went Wrong With the FISA Court*, and we argue that it was erroneous. We conclude that such surveillance requires a warrant in order to be reasonable under the Fourth Amendment. Goitein & Patel, *supra* note 88, at 39-39. Of course, when the U.S. government is taking action overseas, issues of territorial jurisdiction and sovereignty arise, and it may not be possible for the U.S. to execute a warrant issued by a U.S. magistrate judge. Nonetheless, the Fourth Amendment's reasonableness requirement should still apply when one of the communicants is a U.S. person. *Cf.* U.S. v. Stokes, 726 F. 3d 880 (7th Cir. 2013) (applying a reasonableness test to the extraterritorial search of a citizen's property); In re Terrorist Bombings of U.S. Embassies in E. Africa, 552 F.3d 157, 171 (2d Cir. 2008) (same). The proper way to discharge this obligation is again beyond the scope of this report, but for illustrative purposes, it might entail a probable cause finding in combination with a multilateral agreement or cooperation with foreign officials for execution of the search.

90 Defense Intelligence Agency, Intelligence Law Handbook, Defense HUMINT Service, CC-0000-181-95 at § II(3-7)(b) (Aug. 2004), *available at* https://www.aclu.org/files/assets/eo12333/DIA/Intelligence%20Law%20Handbook%20Defense%20HUMINT%20Service.pdf; *See also* Alex Abdo, *New Documents Shed Light on One of the NSA's Most Powerful Tools,* ACLU (Sept. 29, 2014), https://www.aclu.org/blog/new-documents-shed-light-one-nsas-most-powerful-tools.

91 The handbook's discussion of "collection" appears to refer to a version of DoD 5240.1-R enacted on April 25, 1988, and retracted on August 27, 2007. *See* Dep't of Defense, DoD Intelligence Activities, DoD 5240.01 (Aug. 27, 2007), *available at* http://www.dtic.mil/whs/directives/corres/pdf/524001p.pdf. It quotes the definition of "collection" in that version as follows: "[information is 'collected'] … only when it has been received for use by an employee of a DoD intelligence component in the course of his official duties … (and) an employee takes some affirmative action that demonstrates an intent to use or retain the information." *Id.* at § II(3-7)(a) (emphasis added). While that version was retracted, the handbook's general point that the definition of "collection" has a multi-layered and highly technical meaning applies equally to the version of DoD 5240.1-R that is in place today, as discussed *infra*. Moreover, despite the retraction, the NSA's definition of "collection" under USSID 18 appears consistent with the definition contained in the 1988 directive. The 1988 directive's definition of "collection" is also shared by several other agencies, including the Department of Homeland Security, *see* Memorandum from Charles E. Allen, *supra* note 70; the Coast Guard, *see* Coast Guard Intelligence Activities *supra* note 70, at Glossary 2; and the Department of Energy, *see* Dep't of Energy, Department of Energy Procedures for Intelligence Activities § VI(2) (Oct. 19, 1992), *available at* https://www.directives.doe.gov/related-items/doe-procedures-for-intelligence-activities/.

92 DoD USP Procedures, *supra* note 72, at § C.2.2.1. Interception also has a similarly counterintuitive meaning. *Id.* at § C.5.3.2.2.

93 NSA PPD-28 Procedures, *supra* note 81, at § 6.1.; *see also* USSID 18, *supra* note 63, at annex A app. 1 § 2(g) ("Processed or processing means any step necessary to convert a communication into an intelligible form intended for human inspection.").

94 DoD USP Procedures, *supra* note 72, at § C.2.3.

95 USSID 18, *supra* note 73, at § 9.11.

96 USSID 18, *supra* note 73, at § 9.2.

97 Section 9.14 of USSID 18 defines selection as the "insertion of a REDACTED, REDACTED, telephone number, email address, REDACTED into a computer scan dictionary or manual scan guide for the purpose of identifying messages of interest and isolating them for further processing." USSID 18, *supra* note 73, at § 9.14 (emphasis in original).

98 Note that, in contrast to EO 12333 and the NSA's U.S. Persons Procedures, FISA regulates "acquisition" (i.e. the gathering of information) rather than "interception" or "collection." *See* 50 U.S.C. § 1801(f).

99 Audio recordings of these conversations are stored in a "30-day rolling buffer that clears the oldest calls as new ones arrive," and the NSA reportedly listens to "only a fraction of 1 percent" of these calls. The Agency could argue that, since it has not listened to the overwhelming majority of these calls (or selected them for listening), it has not performed any activity that would fall within its definition of "collection." Gellman & Soltani, *NSA Surveillance Program Reaches, supra* note 22.

100 PPD-28, *supra* note 79, at § 2 n.5.

101 *Id.* at § 2.

102 *Id.* at § 2 n.5.

103 *Id.*

104 *Id.* at § 1.

105 *Id.* at § 1(a).

106 *Id.* at § 1(b).

107 *Signals Intelligence,* Nat'l Sec. Agency (Mar. 2, 2015), https://www.nsa.gov/sigint/.

108 PPD-28, *supra* note 79, at n.3.

109 For instance, U.S. government agencies have been criticized for conducting domestic surveillance operations on the express assumption that adopting certain religious ideologies and customs (particularly Islamic doctrines and customs) leads to terrorist violence. Multiple empirical have debunked this assumption as simplistic and inaccurate. *See generally* Faiza Patel, Brennan Ctr for Justice, Rethinking Radicalization (2011), *available at* http://www.brennancenter.org/sites/default/files/legacy/RethinkingRadicalization.pdf. PPD-28's prohibition does not provide insight into whether such an assumption would be a permissible basis for foreign intelligence surveillance, despite the anti-discrimination and religious freedom interests at stake. In the past, the FBI has planted informants in mosques to gather information about the religious practices and political beliefs of their congregations, and created demographic profiles of neighborhoods with large Muslim populations to "help set investigative goals." Michael Isikoff, *Investigators: The FBI Says, Count the Mosques,* Newsweek (Feb. 2, 2003), http://www.newsweek.com/investigators-fbi-says-count-mosques-140311; *see generally Informants,* Al Jazeera (2014), http://webapps.aljazeera.net/aje/custom/2014/fbiinformants/. In the same vein, the NYPD has also planted informants in several mosques and Muslim student groups, and sent undercover officers into Muslim neighborhoods without suspicion of wrongdoing. *See Highlights of AP's Pulitzer Prize-Winning Probe into NYPD Intelligence Operations,* Associated Press (2012), http://ap.org/media-center/nypd/investigation. The unfair targeting of Muslim communities is often motivated by flawed theories of how Americans — particularly American Muslims — are "radicalized" to violence. For example, the NYPD published a study suggesting that various forms of religious behavior, including regular attendance at a Salafi mosque or wearing traditional Islamic clothing, were indicators of radicalization. Mitchell D. Silber & Arvin Bhatt, N.Y.C. Police Dep't, Radicalization in the West: the Homegrown Threat 33 (2007), *available at* https://www.brennancenter.org/sites/default/files/legacy/Justice/20070816.NYPD.Radicalization.in.the.West.pdf. To be sure, the NYPD clarified that "behaviors associated with a greater degree of religiosity, *in and of themselves*, cannot be used as a signature of someone potentially becoming a terrorist" (emphasis added), the biases reflected in the report continue to inform law enforcement attitudes towards American Muslims. *Id.* at 12. The FBI has not explicitly singled out certain religious behaviors as indicators of radicalization, but it has stated that religious conversion and a "commitment to another form of the religion" are symptoms of "preradicalization." Carol Dyer et al., *Countering Violent Islamic Extremism,* FBI Law Enforcement Bulletin, Dec. 2007, at 3, 5, *available at* https://leb.fbi.gov/2007-pdfs/leb-december-2007.

110 PPD-28, *supra* note 79, § 1(c).

111 *Id.* at § 1 n.4; *see also* NSA PPD-28 Procedures, *supra* note 81, at § 3.4.

112 Jonathan Watts, *NSA Accused of Spying on Brazilian Company Petrobras,* Guardian (Sept. 9, 2013), http://www.theguardian.com/world/2013/sep/09/nsa-spying-brazil-oil-petrobras; *see also NSA Documents Show United States Spied Brazilian Oil Giant,* Fantástico (Sept. 8, 2013), http://g1.globo.com/fantastico/noticia/2013/09/nsa-documents-show-united-states-spied-brazilian-oil-giant.html.

113 These policy calculations may well be highly fact-specific and difficult to explore at length in a general directive like PPD-28. Nonetheless, some combination of meaningful and publicly available criteria and robust oversight mechanisms could help to ensure the scope of commercial information obtained is commensurate with a valid and sufficiently specified national security interest.

114 PPD-28, *supra* note 79, § 1(d).

115 The DoD 's U.S. persons procedures, for example, states that DoD intelligence components are authorized to "collect" private communications and information concerning U.S. persons only if less invasive methods (like getting the information from public or diplomatic sources) are not "feasible or sufficient." DoD USP Procedures, *supra* note 72, at § C.2.4. PPD-28 arguably extends this principle to information gathering as well, and certainly extends it to all "collection" activities that affect non-U.S. persons. NSA PPD-28 Procedures, *supra* note 81, at § 3.5.

116 PPD-28, *supra* note 79, § 2; NSA PPD-28 Procedures, *supra* note 81, at § 5.2.

117 ACLU v. Clapper, 785 F.3d 787 (2d Cir. 2015).

118 *Id.* at 801.

119 Jennifer Daskal, *The Substance of the Second Circuit on 215: Four Key Takeaways,* Just Sec. (May 8, 2015), http://justsecurity.org/22875/substance-circuit-215-key-takeaways/.

120 Privacy and Civil Liberties 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 146 (Jan. 23, 2014), *available at* https://www.pclob.gov/library/215-Report_on_the_Telephone_Records_Program.pdf; Richard A. Clarke et al., Liberty and Security in a Changing World, Report and Recommendations of the President's Review Group on Intelligence and Communications Technologies 104 (Dec. 12, 2013), *available at* https://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf.

121 For example, federal criminal law defines terrorism as, among other things, criminal or violent acts intended to "intimidate or coerce" a civilian population or the government. 18 U.S.C. § 2331(1)(B)(i). For immigration purposes, however, anyone who has used an "explosive, firearm or other weapon or dangerous device" other than for "personal monetary gain," and with intent to endanger another person's safety or cause "substantial damage" to property, has engaged in "terrorist activity" and is barred from entering the U.S. 8 U.S.C. § 1182(a)(3)(B)(iii)(V). Some commentators have observed that, this expansive definition, when taken to its logical conclusion, would cover "anyone who's committed an armed crime for a reason other than money." Juliet Lapidos, *Is Nidal Malik Hasan a "Terrorist"?,* Slate (Nov. 11, 2009), http://www.slate.com/articles/news_and_politics/explainer/2009/11/is_nidal_malik_hasan_a_terrorist.html.

122 18 U.S.C §§ 2339A–B; *see also* Holder v. Humanitarian Law Project, 561 U.S. 1 (2010).

123 Charlie Savage et al., *Hunting for Hackers, N.S.A. Secretly Expands Internet Spying at U.S. Border,* N.Y. Times (June 4, 2015), http://www.nytimes.com/2015/06/05/us/hunting-for-hackers-nsa-secretly-expands-internet-spying-at-us-border.html.

124 *Secret Documents Reveal N.S.A. Campaign Against Encryption,* N.Y. Times (2013), http://www.nytimes.com/interactive/2013/09/05/us/documents-reveal-nsa-campaign-against-encryption.html (excerpts from a classified National Security Agency 2013 Budget Request); Bruce Schneier, *Internet Subversion,* Schneier on Sec. (May 12, 2014), https://www.schneier.com/blog/archives/2014/05/internet_subver.html.

125 USSID 18, *supra* note 73, at § 5.1.

126 *Id.* at § 5.1(a) (emphasis in original).

127 *Id.* at § 5.1(c) (emphasis in original).

128 Exec. Order No. 12,333 § 3.5(e), 3 C.F.R. 200 (1981).

129 Declassified Presentation, Office of Gen. Counsel, Nat'l Sec. Agency, *supra* note 1, at Slide 48.

130 Robert Litt, General Counsel, Office of the Dir. of Nat'l Intelligence, Remarks at the Brookings Institute (Feb. 4, 2015) [hereinafter Robert Litt Remarks] (transcript available at IC on the Record), http://icontherecord.tumblr.com/post/110099240063/video-odni-general-counsel-robert-litt-speaks-on.

131 According to Litt, these requirements are broadly reflected in the Worldwide Threat Assessment. *Id.*; *See also* James R. Clapper, Worldwide Threat Assessment of the US Intelligence Community (Feb. 26, 2015), *available at* http://www.dni.gov/files/documents/Unclassified_2015_ATA_SFR_-_SASC_FINAL.pdf.

132 Robert Litt Remarks, *supra* note 120.

133 *Id.*

134 *See* Brennan Ctr for Justice, Strengthening Intelligence Oversight (2015), *available at* https://www.brennancenter.org/sites/default/files/publications/Church_Committee_Web_REVISED.pdf.

135 Robert Litt Remarks, *supra* note 130.

136 *Id.*

137 NSA PPD-28 Procedures, *supra* note 81, § 4.2.

138 International Covenant on Civil and Political Rights, Dec. 16, 1966, S. Exec. Rep. 102-23, 999 U.N.T.S. 171.

139 See *supra* text accompanying notes 105-113, 123.

140 USSID 18, *supra* note 73, at § 5.1.

141 *Id.* at § 6.1(a)(1).

142 Human Rights Watch & American Civil Liberties Union, With Liberty To Monitor All: How Largescale US Surveillance Is Harming Journalism, Law And American Democracy 31 (2014), *available at* http://www.hrw.org/sites/default/files/reports/usnsa0714_ForUPload_0.pdf ("A significant number of journalists reported using various forms of encryption software for their communications with sources or colleagues."); *Id.* at 63 ("As a result of their growing concerns about surveillance, several attorneys reported encrypting their email or other forms of electronic communications.").

143 Sanger & Perlroth, *supra* note 27 ("Google . . . is encrypting more data as it moves among its servers and helping customers encode their own emails. Facebook, Microsoft and Yahoo are taking similar steps.").

144 *NSA Spying Scandal*, Spiegel Online, http://www.spiegel.de/international/germany/bild-1010361-793528.html (excerpt of an untitled leaked NSA document).

145 *See supra* note 24 and accompanying text.

146 Human Rights Watch & American Civil Liberties Union, *supra* note 142, at 39.

147 The data retention limits established under the Intelligence Authorization Act for FY 2015 do not define the term "retention." EO 12333's U.S. persons procedures, however, establish a very specific definition of the term. According to DoD 5240.1-R, data retention is the "maintenance of information about United States persons that can be retrieved by reference to the person's name or other identifying data." DoD USP Procedures, *supra* note 72, at § C.3.2. In other words, the storage of data of or about U.S. persons where their identifying information has been deleted or otherwise masked (for example, replacing Jane Doe with "U.S. PERSON") would not be considered retention that is subject to regulation. This definition of "retention" presumably also applies to PPD-28's restrictions on the retention of non-U.S. persons' information.

148 Where U.S. persons' information is collected under FISA, the rules for retention and dissemination are set forth in FISA court-approved procedures. 50 U.S.C. § 1801(h).

149 Intelligence Authorization Act for Fiscal Year 2015, Pub. L. No. 113-293, § 309 (2014).

150 PPD-28, *supra* note 79, § 4(a)(i).

151 For 5-year limit on retention of U.S. persons' information, see USSID 18, *supra* note 73, § 6.1(a)(1); Intelligence Authorization Act for Fiscal Year 2015, Pub. L. No. 113-293, § 309 (2014). For 5-year limit on retention of non-U.S. persons' information, see NSA PPD-28 Procedures, *supra* note 81.

152 Intelligence Authorization Act for Fiscal Year 2015, Pub. L. No. 113-293, § 309(b)(3)(B)(i) (2014).

153 *Id.* at § 309(b)(3)(B)(ii).

154 *Id.* at § 309(b)(3)(B)(iii).

155 *Id.* at § 309(b)(3)(B)(iv).

156 *Id.* at § 309(b)(3)(B)(v).

157 USSID 18, *supra* note 73, at §§ 6.1(b), 7.2(c)(6) (emphasis added).

158 Intelligence Authorization Act for Fiscal Year 2015, Pub. L. No. 113-293, § 309(b)(3)(B)(vi) (2014).

159 *Id.* at § 309(b)(3)(B)(vii).

160 USSID 18, *supra* note 73, at § 6.1(a)(1).

161 For example, the prevention of wildlife poaching and the theft of cultural properties are identified as foreign intelligence priorities in the DNI's Worldwide Threat Assessment. Clapper, *supra* note 131, at 9; *see also supra* text accompanying note 131. But it would be a stretch to argue that these are U.S. national security concerns.

162 The relevant intelligence official is required to certify in writing: (i) the reasons extended retention is necessary to protect U.S. national security; (ii) the duration for which retention is authorized; (iii) the particular information to be retained; and (iv) the measures the retaining agency is taking to "protect the privacy interests of United States persons or persons located inside the United States." Intelligence Authorization Act for Fiscal Year 2015, Pub. L. No. 113-293, § 309(b)(3)(B)(vii) (2014).

163 PPD-28, *supra* note 79, at § 4.

164 *Id.* at § 4(a)(i).

165 In general, all nonpublic communications containing non-U.S. persons' information may be retained for up to five years. The exceptions to this rule, while worded differently, are just as broad as those pertaining to U.S. persons. For example, non-U.S. persons' information may be retained for more than five years if the appropriate intelligence official determines that "continued retention is in the national security interests of the United States." NSA PPD-28 Procedures, *supra* note 81, at § 6.1(a). The NSA's PPD-28 procedures also preserve the troubling distinction between enciphered and unenciphered communications. Information that is encrypted, believed to "conceal[] secret meaning" or otherwise unintelligible because of an "unknown communication method[]" is not subject to the five-year retention limit until "the information has been made intelligible." *Id.*

166 Charlie Savage, *Obama Administration Set to Expand Sharing of Data That N.S.A. Intercepts,* N.Y. Times (Feb. 25, 2016), *available at* http://www.nytimes.com/2016/02/26/us/politics/obama-administration-set-to-expand-sharing-of-data-that-nsa-intercepts.html?emc=edit_th_20160226&nl=todaysheadlines&nlid=59233787.

167 USSID 18, *supra* note 73, at § 7.2 (emphasis added). Note that, in general, DoD intelligence components including the NSA may disseminate U.S. persons' information gathered under EO 12333 if they have a "reasonabl[e] belie[f]" that the recipient needs the information for a "lawful governmental function." DoD USP Procedures, *supra* note 72, at § C.4.2.2. Potential recipients include DoD employees and contractors; federal, state, and local law enforcement; other intelligence agencies; and foreign governments. *Id.*

168 To be sure, not all of the examples specified in the NSA's U.S. Persons Procedures are equally expansive. For example, the NSA's ability to share information indicating that a U.S. person is a "FOREIGN POWER or AGENT OF A FOREIGN POWER," or that is "pertinent" to the safety of "TARGETS, victims or hostages of INTERNATIONAL TERRORIST organizations," appear to be reasonably tailored to intelligence objectives. USSID 18, *supra* note 73, at §§ 7.2(c)(1), 7.2(c)(6).

169 USSID 18, *supra* note 73, at § 7.2(c)(6).

170 *See supra* Part III.A–B.

171 *See* Memorandum of Understanding: Reporting of Information Concerning Federal Crimes § VII(A) (1995), *available at* http://fas.org/irp/agency/doj/mou-crimes.pdf.

172 *Id.* at § VII(A)(3)(d).

173 *Id.* at § VII(A)(4).

174 *Id.* at § VII(A)(5). Information about the criminal possession of "user quantities" of drugs is not shareable.

175 David Ingram & John Shiffman, *U.S. Defense Lawyers to Seek Access to DEA Hidden Intelligence Evidence,* Reuters (Aug. 8, 2013), http://www.reuters.com/article/us-dea-irs-idUSBRE9761AZ20130808; John Shiffman & Kristina Cooke, *Exclusive: U.S. Directs Agents to Cover Up Program Used to Investigate Americans,* Reuters (Aug. 5, 2013), http://www.reuters.com/article/us-dea-sod-idUSBRE97409R20130805.

176 Although prosecutors reportedly avoid using EO 12333-gathered information as *direct* evidence in criminal proceedings, it has been reported that the government takes the position that prosecutors need not give notice to defendants when they use evidence *derived* from such information. Charlie Savage, *Reagan-Era Order on Surveillance Violates Rights, Says Departing Aide,* N.Y. Times (Aug. 13, 2014), http://www.nytimes.com/2014/08/14/us/politics/reagan-era-order-on-surveillance-violates-rights-says-departing-aide.html; *see also* Patrick C. Toomey, *Executive Order 12333, Notice, and the Due Process Rights of Criminal Defendants,* Just Sec. (Aug. 14, 2014, 2:38 PM), http://justsecurity.org/14040/executive-order-12333-notice-due-process-rights-criminal-defendants/. This suggests that prosecutors are in fact relying on evidence that can ultimately be traced back to EO 12333 surveillance.

177 USSID 18, *supra* note 73, at § 7.2.

178 NSA PPD-28 Procedures, *supra* note 81, at § 7.2.

179 Office of the Dir. of Nat'l Intelligence, Safeguarding the Personal Information of All People, A Status Report on the Development and Implementation of Procedures Under Presidential Policy Directive 28 at 5 (July 2014), *available at* http://fas.org/irp/dni/ppd28-status.pdf.

180 NSA PPD-28 Procedures, *supra* note 81, at § 7.2.

181 Office of the Dir. of Nat'l Intelligence, Foreign Disclosure and Release of Classified National Intelligence, ICD 403 § E(1) (Mar. 13, 2013) [hereinafter ICD 403], *available at* http://www.dni.gov/files/documents/ICD/ICD403.pdf.

182 Office of the Dir. of Nat'l Intelligence, Criteria for Foreign Disclosure and Release of Classified National Intelligence, ICPG 403.1 § (D)(1) (Mar. 13, 2013) [hereinafter ICPG 403.1], *available at* http://www.dni.gov/files/documents/ICPG/ICPG403-1.pdf.

183 *See* discussion *supra* Part IV.B.

184 *See* discussion *supra* Part IV.C.

185 *Id.* at § (D)(2); ICD 403, *supra* note 171, at § E(6)(a).

186 ICPG 403.1, *supra* note 172, at § D(2).

187 Memorandum of Understanding Between the National Security Agency/Central Security Service (NSA/CSS) and the Israeli SIGINT National Unit (ISNU) Pertaining to the Protection of U.S. Persons § IV(b)(2), *available at* http://www.theguardian.com/world/interactive/2013/sep/11/nsa-israel-intelligence-memorandum-understanding-document.

188 *Id.* at § IV(b)(4).

189 *Id.* at § IV(b)(5).

190 *Id.* at § IV(a)(2).

191 *Id.* at § IV(a).

192 *Id.* at § V(a).

193 Letter from James R. Clapper, Dir. Nat'l Intelligence, to Bd. of Dirs., Amnesty Int'l (Sept. 5, 2015) (on file with authors).

194 Peter Beaumont, *Israeli Intelligence Veterans Refuse to Serve in Palestinian Territories,* Guardian (Sept. 12, 2014), http://www.theguardian.com/world/2014/sep/12/israeli-intelligence-reservists-refuse-serve-palestinian-territories.

195 James Bamford, *Israel's N.S.A. Scandal,* N.Y. Times (Sept. 16, 2014), http://www.nytimes.com/2014/09/17/opinion/israels-nsa-scandal.html?_r=0.

196 USSID 18, *supra* note 73, at App. 1 Annex 1 § 8(b). For example, under a program codenamed TEMPORA, GCHQ taps into huge volumes of the world's Internet data that passes through fiber optic cables located on U.K. territory, and sifts and analyzes such data with the help of the NSA. Such data potentially contains Americans' phone calls, e-mails, Facebook chats and web browsing histories. Ewan MacAskill et al., *GCHQ Taps Fibre-Optic Cables for Secret Access to World's Communications,* Guardian (June 21, 2013), http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa.

197 USSID 18, *supra* note 73, at App. 1 Annex 1 § 8(a).

198 *Id.* at App. 1 Annex 1 § 8(c).

199 50 U.S.C. § 1801(e)(2).

200 USSID 18, *supra* note 73, at App. 1 Annex 1 § 8(d).

201 *Id.*

202 To be sure, the full extent to which Congress can place substantive restrictions on surveillance activities conducted pursuant to the President's authority as Commander-in-Chief is unclear. However, it is well established that Congress has a duty to oversee the intelligence community's compliance with internal rules and procedures, the relevant U.S. laws, and the Constitution.

203 50 U.S.C. § 3093(a)(1).

204 50 U.S.C. § 3093(c)(2). The "Gang of Eight" comprises the leaders and ranking members of both intelligence committees, and the majority and minority leaders of the House and Senate.

205 50 U.S.C. § 3093(e)(1) (emphasis added).

206 Marshall Curtis Erwin, Cong. Research Serv., 7-5700, "Gang of Four" Congressional Intelligence Notifications 1 (Apr. 16, 2013), *available at* http://fas.org/sgp/crs/intel/R40698.pdf.

207 *Id.* at 7 (quoting "letter from Representative Jane Harman to President George W. Bush, January 4, 2006, regarding the National Security Agency (NSA) electronic communications surveillance program, often referred to as the Terrorist Surveillance Program, or TSP").

208 50 U.S.C. § 3093(b). However, the accompanying congressional report states that the phrase "exceptionally sensitive matters" refers to "extremely sensitive categories of classified information such as information concerning the operational details of military deployments, and extraordinarily sensitive diplomatic contacts" that the intelligence committees would not "routinely require to satisfy their responsibilities." S. Rep. No. 102-85, at 33 (1991), *reprinted in* 1991 U.S.C.C.A.N. 193, 226 (accompanying S. 1325, 102nd Cong. (1991), which authorized FY1991 Intelligence appropriations).

209 Press Release, Sen. Dianne Feinstein, Feinstein Statement on Intelligence Collection of Foreign Leaders (Oct. 28, 2013), *available at* http://www.feinstein.senate.gov/public/index.cfm/press-releases?ID=61f9511e-5d1a-4bb8-92ff-a7eaa5becac0.

210 S. Rep. No. 114-8, at § III(B)(3) (2015) ; *See also* Eli Lake, *Congress Scouring Every U.S. Spy Program,* Daily Beast (Oct. 10, 2014, 5:45 AM), http://www.thedailybeast.com/articles/2014/10/10/congress-scouring-every-u-s-spy-program.html.

211 Office of the Dir. of Nat'l Intelligence, *The U.S. Intelligence Community Budget,* IC on the Record (Feb. 9, 2016), http://icontherecord.tumblr.com/ic-budget; Office of the Dir. of Nat'l Intelligence, 2014 Report on Security Clearance Determinations (Apr. 2015), *available at* http://fas.org/sgp/othergov/intel/clear-2014.pdf; *see also Intelligence Budget Data,* FAS Intelligence Resource Program, http://fas.org/irp/budget/; Brennan Ctr. for Justice, *supra* note 124, at 5.

212 Brennan Ctr for Justice, *supra* note 134, at 5.

213 Alexander W. Joel, *The Truth about Executive Order 12333,* Politico (Aug. 18, 2014), http://www.politico.com/magazine/story/2014/08/the-truth-about-executive-order-12333-110121.html.

214 Privacy and Civil Liberties Oversight Board, PCLOB Examination of E.O. 12333 Activities in 2015, https://www.pclob.gov/library/20150408-EO12333_Project_Description.pdf.

215 Margo Schlanger, *Intelligence Legalism and the National Security Agency's Civil Liberties Gaps*, 6 Harv. Nat. Sec. J. 112, 173 (2015), *available at* http://harvardnsj.org/wp-content/uploads/2015/02/Schlanger.pdf.

216 *Id.* at 185.

217 *Id.* at 184.

218 Shirin Sinnar, *Protecting Rights from Within? Inspectors General and National Security Oversight*, 65 Stan. L. Rev. 1027, 1076-77 (2013), *available at* http://law.stanford.edu/wp-content/uploads/sites/default/files/publication/429572/doc/slspublic/Sinnar_65_Stan._L._Rev._1027.pdf. Relatedly, the capacity of internal oversight offices to constrain agencies may also be limited by internal political pressures, such as the fear of "losing influence and being ignored" (especially among more mission-oriented colleagues), and the natural inclination to "get along with colleagues and to earn their approbation." See Schlanger, *supra* note 215, at 193, 196.

219 Home Bldg. & Loan Ass'n v. Blaisdell, 290 U.S. 398, 426 (1934).

220 *See* Johnson v. United States, 333 U.S. 10, 14 (1948). The Court observed that the Fourth Amendment protection "consists in requiring that [evidentiary] inferences be drawn by a neutral and detached magistrate instead of being judged by the officer engaged in the often competitive enterprise of ferreting out crime." *Id.* The same can be said for intelligence operations.

221 *Id.*

222 Such documents would include: (1) FISC or the Office of Legal Counsel ("OLC") opinions and memoranda that consider whether and how the Fourth Amendment applies to the acquisition of: (a) non-U.S. persons' communications on U.S. soil; (b) one-end foreign radio communications transiting U.S. territory; and (c) U.S. persons' communications overseas while conducting intelligence surveillance operations that do not target U.S. persons; (2)FISC or OLC opinions and memoranda that interpret the scope and nature of Article II's limits on the power of the President to conduct foreign intelligence surveillance (in addition to the information provided on such interpretations in the May 6, 2004 Memo entitled "Review of the Legality of the STELLAR WIND Program," https://www.aclu.org/sites/default/files/assets/olc_stellar_wind_memo_-_may_2004.pdf); and (3) State Department or OLC opinions and memoranda that interpret the scope of the right to privacy under Article 17 of the International Covenant on Civil and Political Rights, the freedom of expression under Article 19 of the ICCPR, and the right to an effective remedy for human rights violations under Article 2(3) of the ICCPR. International Covenant on Civil and Political Rights, Dec. 16, 1966, S. Exec. Rep. 102-23, 999 U.N.T.S. 171.

STAY CONNECTED TO THE BRENNAN CENTER

Visit our website at **www.brennancenter.org.**
Sign up for our electronic newsletters at **www.brennancenter.org/signup.**

Latest News | Up-to-the-minute information on our work, publications, events, and more.

Voting Newsletter | Latest developments, state updates, new research, and media roundup.

Justice Update | Snapshot of our justice work and latest developments in the field.

Fair Courts | Comprehensive news roundup spotlighting judges and the courts.

Money in Politics | Latest state and national developments and original analysis.

Redistricting Round-Up | Analysis of current legal battles and legislative efforts.

Liberty & National Security | Updates on privacy, government oversight, and accountability.

Twitter | www.twitter.com/BrennanCenter
Facebook | www.facebook.com/BrennanCenter
Instagram | www.instagram.com/BrennanCenter

NEW AND FORTHCOMING BRENNAN CENTER PUBLICATIONS

Stronger Parties, Stronger Democracy: Rethinking Reform
Daniel I. Weiner and Ian Vandewalker

Candidates and Super PACs: The New Model in 2016
Brent Ferguson

State Options for Reform
Brent Ferguson

America's Voting Machines at Risk
Lawrence Norden and Christopher Famighetti

The Case for Automatic, Permanent Voter Registration
Brennan Center for Justice

Crime in 2015: A Preliminary Analysis
Matthew Friedman, Nicole Fortier, and James Cullen

Solutions: American Leaders Speak Out on Criminal Justice
Inimai Chettiar, Michael Waldman, Nicole Fortier, and Abigail Finkelman

Legal Change: Lessons from America's Social Movements
Jennifer Weiss-Wolf and Jeanine Plant-Chirlin

For more information, please visit www.brennancenter.org.

BRENNAN
CENTER
FOR JUSTICE
TWENTY
YEARS

at New York University School of Law

161 Avenue of the Americas
12th Floor
New York, NY 10013
646-292-8310
www.brennancenter.org