A HOOVER INSTITUTION ESSAY

Trends and Predictions in Foreign Intelligence Surveillance

THE FAA AND BEYOND

DAVID S. KRIS

Aegis Paper Series No. 1601

It is a strange time for national security. Beginning in 2013, Edward Snowden's leaks caused the US government to significantly reduce the scope, and increase the transparency, of its foreign intelligence surveillance, while the president urged caution and restraint in response to the extraordinary rise of the Islamic State of Iraq and the Levant (ISIL). At the same time, US communications providers sought additional reforms and reduced their cooperation with surveillance directives in important cases. Finally, anti-surveillance politicians, on the right and left of the US political spectrum, prospered as part of a burgeoning populist movement. In Western Europe, by contrast, ISIL's rise spurred a significant and overt expansion of surveillance authorities. European governments, particularly the United Kingdom, began making increasingly strident demands for communications data from US providers. And the European Union struck down the safe-harbor regime for trans-Atlantic data sharing on the grounds that US surveillance laws do not adequately protect privacy. Despite increased transparency, as of January 2016, the immense technical and legal complexity of US surveillance law continues to challenge informed debate across all of these fronts.

In this highly charged and confused environment, Congress will soon take up the Foreign Intelligence Surveillance Act (FISA) Amendments Act (FAA), which is set to expire at the end of 2017. I make six predictions about the issues likely to dominate that legislative process. Most of those issues concern incremental change, and a range of possible outcomes well within existing legal and policy paradigms; many are explained in a 2014 report by the Privacy and Civil Liberties Oversight Board (PCLOB). All of the following issues are important: the "upstream" collection of communications about non-US persons located abroad (less than 10 percent of FAA collection, and probably unavoidable for technical reasons); US person queries of FAA data (fewer than 200 conducted by NSA in 2013, more by other agencies); statutorily required or forbidden sharing of raw FAA data with foreign partners (now dealt with through FISA Court-approved minimization procedures); the authorized purposes of FAA collection (likely not to affect existing collection very much); and NSA compliance issues (already well publicized, dealt with by the court and congressional

This paper was completed and first submitted for prepublication review on December 8, 2015, and then edited, resubmitted, and finally cleared in its present form on February 8, 2016. I am grateful to the participants in the Hoover Institution's conference, The Next Wave of Surveillance Reform, for their helpful comments.

oversight, and unlikely to result in significant FAA amendments, but perhaps significant for the long run as the intelligence community moves data to the cloud). But they are unlikely to have a revolutionary effect on security or privacy, except perhaps in the aggregate. The one exception concerns surveillance under Executive Order 12333, which is very likely to arise in connection with FAA renewal, but is difficult to discuss at present because it is the subject of a forthcoming report from the PCLOB.

I also make predictions about political and technological trends that I think will have the biggest impact on surveillance in the longer run. These predictions are more speculative than the ones discussed above. They include increasing pressure on FISA's "technical assistance" provisions, partly due to challenges posed by widespread and varied encryption; two gaps in US law resulting from outdated assumptions that providers will voluntarily cooperate when surveillance requests are certified as lawful but compliance is not compelled; a growing but so far unmet need for international agreements to resolve cross-border data requests; the increasing indeterminacy of location on the Internet and the resulting foundational threat to US surveillance law; the Internet of Things and "fintech," which promise to pose a host of practical, legal, and cultural challenges; and the increasing availability of open source and social media, which creates significant problems and opportunities for US intelligence and counter-intelligence. At present, I fear that most of these issues, with the possible exception of cross-border data requests, are not very well in focus at the highest levels of the executive and legislative branches. But I believe that they should be considered soon, either in connection with FAA renewal or in a separate process, because they have the potential to cause significant change over the next several years.

• • •

Technological and political developments in the next few years will have a major impact on US national security and the law that governs it, including surveillance law. Part 1 of this paper provides historical background for the discussion of those developments, beginning with the Foreign Intelligence Surveillance Act (FISA) Amendments Act (FAA) in 2008, but focused particularly on developments since mid-2013. Part 2 presents six issues that I think are most likely to arise in connection with a legislative extension of the FAA, which is otherwise set to expire at the end of 2017. These issues are already well in focus, largely due to reports from the Privacy and Civil Liberties Oversight Board (PCLOB), and should persist absent major disruption, such as a significant terrorist attack on the United States, or perhaps the result of our 2016 presidential election. With one possible exception, concerning Executive Order 12333, these issues concern only incremental change and fit comfortably within existing legal and policy paradigms; although important, they are unlikely to have a profound effect on security or privacy. Part 3 of the paper looks further ahead. It discusses six political and technological trends that I think will have the biggest impact on surveillance in the longer run, and explains why many of them should be considered

now. These longer-term predictions are more speculative, but they concern issues that are potentially far more significant than those addressed in part 2; I hope they will be interesting even if ultimately proven wrong. Part 4 of the paper is a short conclusion.

1. Background

The predictions discussed below make sense only when considered in historical context. Issues likely to arise in connection with the FAA's renewal in 2017, discussed in part 2, require an understanding of the statute's enactment in 2008 and the PCLOB's major report on the law in 2014.[1] The longer-term issues discussed in part 3 make sense only against the turbulent backdrop of the last two or three years, beginning with the first unauthorized disclosure from Edward Snowden in June 2013 and including the rise of the Islamic State of Iraq and the Levant (ISIL).

A. The FISA Amendments Act of 2008

The FISA Amendments Act (FAA) was enacted by Congress in 2008 to address both political and technological changes from the preceding several years. Politically, Congress passed the FAA in response to unauthorized disclosures about the Terrorist Surveillance Program (TSP) ordered by President George W. Bush shortly after the September 11, 2001, attacks. Revealed by the *New York Times* in December 2005, the TSP allowed the National Security Agency (NSA) to acquire the contents of international communications, to or from the United States, when one communicant was suspected of being linked to al Qaeda or related terrorist organizations. Although subject to FISA, surveillance under the TSP did not comply with the statute and generated enormous controversy, centered on the president's power to disregard statutes under Article II of the Constitution. Roughly speaking, the FAA amended FISA to authorize the TSP, although it also reiterated that, as amended, FISA is the "exclusive" means by which such surveillance can be conducted.[2]

Technologically, the FAA "modernized" FISA in response to changing conditions. In particular, the rise of web-based e-mail and other developments made it more difficult to determine the location of parties to an intercepted communication. With FISA's rules so heavily dependent on knowledge of those locations, the statute became difficult to administer; it also required a high level of legal protection for surveillance of e-mail acquired from storage in the United States, even if both sender and recipient were non-US persons, located abroad, with no other connection to this country—something the drafters of FISA clearly did not contemplate in 1978. The FAA's central innovation, in section 702 of the law, was to reduce protections for surveillance targeting non-US persons reasonably believed to be located abroad, regardless of the location of their interlocutors. Section 702 authorized such surveillance without the FISA Court making any finding about the particular person or facility (e.g., an e-mail address) being surveilled.[3]

The FAA profoundly affected the scope of US foreign intelligence surveillance, at least under FISA. In 2014, 92,707 persons were targeted under section 702, up from 89,138 the year before. This compares to 1,562 persons targeted in 2014 under traditional FISA and FAA §§ 703 and 704, up from 1,144 the year before. FAA surveillance covers far more persons than does traditional FISA surveillance.[4]

B. The Snowden Disclosures Lead the United States to Limit Surveillance

The Edward Snowden disclosures, and the government's response to them, had a major effect on US politics and policy, igniting debates about secret law and surveillance excesses and spurring resistance to governmental surveillance from communications providers.[5] The disclosures, which began in June 2013 and continued with the assistance of some very skilled journalists, were quite significant in their own right, showing that the FISA Court had authorized NSA and the Federal Bureau of Investigation (FBI) to collect the records (but not the contents) of a huge number of telephone calls, including domestic calls. The disclosures claimed to reveal many other things, as well, not all of which have been confirmed by the US government.

The disclosures arrived at a time of post-9/11 fatigue. They were preceded, in May 2013, by a speech in which the president announced that while we were still threatened by terrorism, "[t]here have been no large-scale attacks on the United States . . . our homeland is more secure" and "the threat has shifted and evolved from the one that came to our shores on 9/11." He declared that "this war, like all wars, must end," that America was "at a crossroads," and that "the future of terrorism . . . [and] the scale of this threat closely resembles the types of attacks we faced before 9/11." The president also stated in the May 2013 speech that he was "troubled by the possibility that leak investigations may chill the investigative journalism that holds government accountable," and he had directed the attorney general to "convene a group of media organizations to hear their concerns as part of [a] review" of Department of Justice (DOJ) guidelines governing investigations that involve reporters.[6] In short, the president stated shortly before the Snowden disclosures, the terrorist threat was reduced and the government should be less aggressive in response to leaks of classified information.

The president's initial response to Snowden, in June 2013, was to dismiss him as a "twenty-nine-year-old hacker" and publicly to prioritize relations with Russia and China over demands for his extradition:

> [W]e've got a whole lot of business that we do with China and Russia. And I'm not going to have one case of a suspect who we're trying to extradite suddenly being elevated to the point where I've got to start doing wheeling and dealing and trading on a whole host of other issues simply to get a guy extradited, so that he can face the Justice system here in the United States. . . . And I'm sure there will be a made-for-TV movie somewhere down

> the line . . . . But one last thing . . . no, I'm not going to be scrambling jets to get a twenty-nine-year-old hacker.[7]

By August 2013, the government had affirmatively embraced the demand for greater scrutiny generated by the disclosures, with the president asserting that he had in fact "called for a thorough review of our surveillance operations before Mr. Snowden made these leaks." The president explained that he had "never made claims that all the surveillance technologies that have developed since the time some of these laws had been put in place somehow didn't require potentially some additional reforms." In fact, he stated, "That's exactly what I called for" in the May 2013 speech.[8] And while "Mr. Snowden's leaks triggered a much more rapid and passionate response than would have been the case if I had simply appointed [a] review board to go through, and I had sat down with Congress and we had worked this thing through . . . I actually think we would have gotten to the same place."[9]

As those reviews were unfolding, US communications providers continued to push for additional reforms. One of the most prominent and thoughtful advocates in that area was Microsoft, which, through its then-General Counsel Brad Smith, identified a "technology trust deficit" due to the Snowden disclosures and outlined the "unfinished business" required to close it.[10] In part, at least, Microsoft was understandably concerned that, in the absence of visible reform, its European counterparts were enjoying a competitive advantage in the form of perceived relative immunity from surveillance. As Smith put it, "people have real questions and concerns about how their data are protected. These concerns have real implications for cloud adoption. After all, people won't use technology they don't trust. We need to strike a better balance between privacy and national security to restore trust and uphold our fundamental liberties."[11]

One of the key points, Smith explained, was limiting cross-border data requests: "We're concerned about governmental attempts to use search warrants to force companies to turn over the contents of non-US customer communications that are stored exclusively outside the United States."[12] Microsoft ultimately chose to resist a directive issued under the US Stored Communications Act by the DOJ to produce e-mail of a suspected drug dealer on the grounds that the e-mail was stored in Ireland, rather than in the United States.[13] The introduction to its brief in the Second Circuit used informal language capable of being understood by a broader audience than the three-judge panel hearing the case.[14]

By the fall of 2013, the government had made a bold decision to decrease the scope, and increase the transparency, of US foreign intelligence surveillance, recalibrating the balance between security and privacy in favor of the latter. In October, Lisa Monaco, the president's counterterrorism adviser, wrote in *USA Today* of the administration's desire to ensure that "privacy and civil liberties are appropriately protected," promised

"even greater focus to ensuring that we are balancing our security needs with . . . privacy concerns," and committed to "ensure we are collecting information because we *need* it and not just because we *can*."[15] The editorial, which noted with approval the ongoing review of the FAA by the PCLOB, was a powerful statement of the administration's commitment to curtail perceived foreign intelligence surveillance excesses and to emphasize privacy—i.e., to do less surveillance than legally permitted based on policy preferences.

This approach found formal articulation in Presidential Policy Directive-28 (PPD-28) and a speech given by President Obama at the Department of Justice in January 2014. In essence, the government committed to (1) introduce outside advocates into the Foreign Intelligence Surveillance Court (FISC), which was later accomplished in the USA Freedom Act of 2015, (2) adopt more stringent minimization procedures for US person information incidentally collected under FAA § 702, and (3) end bulk collection of telephony metadata, also accomplished in the USA Freedom Act.[16]

It also committed to take what the president termed "the unprecedented step" of adding new protections for non-US persons, including requirements that intelligence surveillance "take into account that all persons should be treated with dignity and respect, regardless of their nationality or wherever they may reside" and recognize the "legitimate privacy and civil liberties concerns of . . . citizens of other nations." Under PPD-28, "[p]rivacy and civil liberties shall be integral considerations in the planning of US signals intelligence activities," including for foreign persons. This makes a stark contrast with the language of Executive Order (EO) 12333, in force since the Reagan administration, which focuses almost exclusively on the privacy interests of US persons.[17] Implementation of PPD-28 remains ongoing as of this writing, but many steps have apparently been taken to limit surveillance and protect foreigners' privacy rights and dignity.[18] One recent paper identified at least two dozen measures undertaken since 2013 to reform surveillance laws and programs.[19] In the fall of 2015, the administration also decided not to support legislation requiring providers to retain access to encrypted communications that they transmit.[20] There is no question but that President Obama and his senior national security advisers have significantly reduced the scope, and increased the transparency, of US foreign intelligence surveillance since mid-2013: it may be their chief legacy in this area.[21]

While the White House was curtailing surveillance and providers were pushing for even more curtailment, anti-surveillance political positions, tied to populism on both the right and the left, were on the rise in the United States.[22] The shift was especially visible in the Republican Party, which witnessed the advent of the Tea Party soon after President Obama's election[23] and, at this writing, features Donald Trump as its leading presidential candidate.[24] Trump is trailed closely by Senator Ted Cruz, despite Cruz's

anti-surveillance positions,[25] for which he has been criticized by other Republican candidates.[26] Few observers during the administration of the last Republican president, George W. Bush, would have predicted this state of affairs. On the Democratic side, Bernie Sanders continues at this writing to enjoy strong standing in his race with Hillary Clinton, despite being one of only sixty-seven members of Congress to have voted against the USA Patriot Act in 2001 (and again in 2011).[27] Of course, it can be difficult to separate the politics of surveillance from broader political trends, and the range of US public opinion on surveillance surely derives in some part from the recent positions of the executive branch, which is often the proponent of more rather than less surveillance. Whatever the causes, however, there is no question but that American politics has over the past few years shifted to embrace more anti-surveillance positions (although the attacks in Paris and San Bernardino have provided some recent counterweight to that shift).

C. ISIL's Rise Leads Europe to Increase Surveillance

During this same period, while the United States was restricting its foreign intelligence surveillance, European governments were expanding their surveillance authorities, in response to growing concerns about ISIL and other terrorist groups. During 2013 and 2014, ISIL rose to power, taking credit for attacks killing eighty-eight people in Iraq in January 2013,[28] announcing its merger with the Syrian Jabhat al-Nusra group in April,[29] orchestrating a large prison break in Iraq in July,[30] and capturing Syrian oil fields in November.[31] In 2014, ISIL took Fallujah in January,[32] directed or inspired an attack on a Jewish museum in Belgium in May,[33] took Mosul and announced a caliphate in June,[34] and released video of the execution of two US journalists in early September[35] and of a UK humanitarian worker later that month.[36] Although the president in early 2014 seemed to dismiss ISIL as unimportant,[37] by later in the year he made clear that ISIL was a significant threat, at least in the Middle East,[38] and focused, at least initially, on regional containment.[39] By late 2015, ISIL had probably recruited at least 4,500 Westerners to its cause, many of them with European passports, and some of whom returned to Europe to conduct attacks.[40]

At the same time, global instability was rising, and failed states like Yemen and Libya created more safe havens for terrorists. From 2013–2015, al Qaeda in the Arabian Peninsula (AQAP) took advantage of instability and proxy fighting between Iran and Saudi Arabia in Yemen. In December 2013, for example, AQAP attacked the Yemeni Ministry of Defense, killing fifty-six people; in September 2014, Houthi rebels took control of Sanaa; in March 2015, President Hadi was forced to flee the country (and later returned); and by April 2015, AQAP had seized the fifth-largest Yemeni city (and "emptied its bank and prison"), an oil terminal, a military base, and an airport in southern Yemen.[41] AQAP also claimed credit for the January 2015 attack on *Charlie Hebdo* in Paris.[42] During this period, Libya also essentially fell into civil war; the United

Nations withdrew in July of that year. By 2015, ISIL had a well-established presence and was reportedly using Libya as a gateway to Europe.[43]

Witnessing these developments in 2014 and 2015, in contrast to the United States, European countries developed new and expanded surveillance authorities.[44] The Council of Europe's Commissioner for Human Rights aptly summarized the situation in October 2015, recounting efforts to expand surveillance authority in France, Germany, Austria, the Netherlands, and Finland (and probably having in mind similar efforts in the United Kingdom and Canada):

> When Edward Snowden disclosed details of America's huge surveillance program two years ago, many in Europe thought that the response would be increased transparency and stronger oversight of security services. European countries, however, are moving in the opposite direction. Instead of more public scrutiny, we are getting more snooping.[45]

Further expansions of European surveillance are likely—such as the UK's remarkable draft Investigatory Powers bill, discussed below.[46]

At this writing, in the aftermath of the Paris and San Bernardino attacks in late 2015, further attacks in the West from ISIL and other terrorist groups seem almost inevitable.[47] Indeed, ISIL's ascendancy represents a significant change in paradigm due to several factors, chief among them that an international terrorist group has now become essentially a state actor, with control of significant territory, large sums of money and income (measured in the hundreds of millions or billions of dollars), and a worldwide strategy that includes a growing focus on external operations and an expanding cadre of geographically dispersed affiliates and allies.[48] As such, particularly due to its oil revenue and thousands of Western recruits, ISIL clearly has far greater resources in materiel and personnel than groups like al Qaeda.[49] Even if ISIL loses control of much of its territory, it is quite unlike any recent international terrorist group (and even if ultimately degraded or defeated, it will leave the Middle East more unstable).[50] It is not hard to imagine ISIL and the West moving into a kind of relatively limited war, with the West bombing but not sending significant numbers of ground troops to ISIL-held territory, and ISIL directing, sponsoring, or inspiring terrorist attacks against the West, at or above the scale seen in Paris and San Bernardino.[51] The wild card in that state of affairs, however, will be whether ISIL is willing and able to engage in strategic terrorism, perhaps involving attacks with weapons of mass destruction.[52]

2. Predictions Concerning Renewal of the FAA

As noted above, the FAA will expire, unless extended, in December 2017. Between now and then, Congress will very likely renew the statute, but only after extensive legislative debate. Many of the issues likely to arise in that debate derive from the PCLOB's report

on FAA § 702. The report generally found the section 702 surveillance program to be valuable, lawful, and appropriate:

> Overall, the Board has found that the information the program collects has been valuable and effective in protecting the nation's security and producing useful foreign intelligence. The program has operated under a statute that was publicly debated, and the text of the statute outlines the basic structure of the program. Operation of the Section 702 program has been subject to judicial oversight and extensive internal supervision, and the Board has found no evidence of intentional abuse.[53]

Based in part on this assessment, and the support for the statute from members of Congress in both political parties, there is very little doubt that the FAA will be renewed, rather than allowed to sunset, when the time comes at the end of 2017.

However, the PCLOB report also recommended several reforms based on its view that "certain aspects of the Section 702 program push the program close to the line of constitutional reasonableness. Such aspects include the unknown and potentially large scope of the incidental collection of US persons' communications, the use of 'about' collection to acquire Internet communications that are neither to nor from the target of surveillance, and the use of queries to search for the communications of specific US persons within the information that has been collected."[54] Between now and the end of 2017, I think the following issues will arise in connection with the FAA's renewal, many of them based on the PCLOB's recommendations.[55] These predictions are not necessarily normative.

A. "Upstream" and "About" Collection

The first question likely to arise in connection with FAA renewal concerns "upstream" collection under section 702, including collection of communications "about," rather than to or from, a surveillance target. As I have explained elsewhere, collection under section 702 "occurs not only directly from Internet service providers (ISPs), but also at certain 'upstream' locations, like international switches or other backbone facilities, as communications transit through them."[56] In other words, section 702 surveillance comes in two varieties: "upstream" collection at the Internet backbone facilities and "downstream" or "PRISM" collection from ISPs or other communications providers. Approximately 90 percent of NSA's FAA § 702 Internet collection is downstream/PRISM collection; less than 10 percent involves upstream.[57]

The "upstream" facilities involved in section 702 surveillance carry huge numbers of communications, including some domestic communications, the metadata and contents of which are scanned to determine whether they contain a targeted selector, such as an e-mail address. That is, NSA collects upstream not only the messages sent to and from

a target's e-mail address, like BadGuy@ISP.com, but also messages sent between non-targets that mention BadGuy@ISP.com (the e-mail address, not merely the name).[58] Indeed, "[b]ecause of the manner in which the NSA conducts upstream collection, and the limits of its current technology, the NSA cannot completely eliminate 'about' communications from its collection without also eliminating a significant portion of the 'to/from' communications that it seeks."[59]

As an unavoidable byproduct of "to/from" collection at the upstream locations, "about" collection can be defended under two publicly available FISA Court decisions from 2011. In those decisions, the court addressed another unavoidable aspect of upstream collection—NSA's acquisition of entire Internet "transactions," which may contain multiple communications, including some communications that are outside the scope of section 702, but which have been bundled together by ISPs or other private-sector companies for business reasons. If an e-mail to or from a lawful surveillance target is bundled in a single transaction with other, unrelated communications, from other individuals, NSA may not be able to avoid acquiring *all* of the communications in the transaction, including the unrelated ones. The FISA Court initially struck down NSA's minimization procedures governing that inevitable over-collection, but later upheld modified procedures that imposed more stringent limits on retention of the unrelated content.[60] The court reached that result despite the large scale of the over-collection: NSA annually acquires "tens of thousands of wholly domestic communications, and tens of thousands of non-target communications of persons who have little or no relationship to the target but who are protected under the Fourth Amendment."[61] The PCLOB likewise found "about" collection tolerable, based primarily on its inevitability as part of "to/from" upstream collection.[62]

In connection with FAA renewal, I expect additional focus on the inevitability, legality, and desirability of "about" collection. The first questions likely to arise will be whether NSA now has the technical ability to parse "about" collection and "to/from" collection, and if not, whether the agency is trying to develop such an ability. (A related question will be whether NSA has developed, or is trying to develop, the ability to separate one individual communication from another within an Internet transaction.) This will be a very technical conversation, and may need to be conducted in closed session. It seems unlikely that NSA has developed such an ability since 2014, in part because one of the main challenges to doing so is the constantly changing nature of commercial Internet protocols, but the questions will need to be asked and answered.[63] Given the state of confusion about the mechanics and other details of upstream collection that persist, it also may be helpful if the legislative debates can further illuminate how the collection works, without compromising national security.

Either way, and especially if "about" collection is no longer inevitable, I expect Congress to consider whether it should be permitted or forbidden by statute (perhaps

against a Fourth Amendment backdrop). Much of the prior focus on "about" collection has concerned retention of the inevitably over-collected data. In connection with FAA renewal, however, I think that Congress may focus more intensively on the collection itself—i.e., on the fact that "NSA's machines scan the contents of *all* of the communications passing through the collection point, and the presence of the selector . . . that justifies the collection is not known until *after* the scanning is complete."[64] This purely legal issue, arguably involving the result of a search being used to justify the search, is both interesting and challenging.

Finally, if "about" collection is retained in the statute, Congress may ask whether it should be expanded or restricted. One possibility for expansion might be to permit "about" collection both upstream and downstream—e.g., allowing the government to direct ISPs to scan their servers for any stored e-mail mentioning BadGuy@ISP.com, as well as e-mails to or from that e-mail address. Even if it were technically feasible, this seems most unlikely. As discussed in greater detail in part 1, the Obama administration since 2013 has consistently supported less surveillance, rather than more, and I doubt that it will push for an expansion here.[65] Nor is the new president likely to push for this after January 2017—at least absent a disruptive event of the sort described in the first paragraph of this paper. Without support from the executive branch, increased "about" collection seems very unlikely, especially given the legal questions it raises. As to further restrictions, there are always a variety of incremental changes Congress could try to legislate, particularly in the area of minimization—e.g., a one-year retention period, rather than the two-year period approved by the FISA Court in 2011.

B. Queries

A second question likely to arise in connection with FAA renewal is the government's authority to query un-minimized FAA § 702 data with US person identifiers, or in other ways designed to return information about US persons.[66] Attentive members of the news media have already identified querying as one of the most likely issues to be addressed.[67] To provide a sense of scale, according to the PCLOB, in 2013, "NSA approved 198 US person identifiers to be used as content query terms" in queries of FAA § 702 data.[68]

Querying raises concerns primarily when US persons are not surveillance targets but have their communications acquired incidentally, during collection targeting others. Roughly speaking, US persons' communications could be collected incidentally under section 702 in any of three ways, two of which apply only to upstream collection: the US person could be the interlocutor of a target, which is inherent in any form of surveillance (including law-enforcement surveillance) that captures both sides of an intercepted conversation; the US person's communication could be acquired upstream as part of "about" collection concerning a targeted selector; or the US person's

communication could be acquired upstream as part of the same Internet "transaction" as a targeted communication.

Given these three possibilities, querying upstream (rather than downstream) data with US person identifiers is plainly more controversial. But NSA's 2014 minimization procedures do not permit it, and neither the FBI nor the CIA has access to un-minimized upstream data.[69] Legislative intervention to address a hypothetical concern seems relatively unlikely, unless it is in connection with broader changes to upstream collection. But it would be possible if Congress does not want to leave the matter to the other two branches of government.

With respect to downstream (PRISM) data, the PCLOB recommended that NSA and CIA minimization procedures "permit the agencies to query collected section 702 data for foreign intelligence purposes using US person identifiers only if the query is based upon a statement of facts showing that it is reasonably likely to return foreign intelligence information as defined in FISA." The PCLOB recommended that the "NSA and CIA should develop written guidance for agents and analysts as to what information and documentation is needed to meet this standard, including specific examples."[70] It appears that the NSA and CIA have implemented this recommendation with the FISA Court's approval,[71] and it is not clear that Congress will demand more by statute.

Two members of the PCLOB recommended in addition that "[e]ach US person identifier should be submitted to the FISA court for approval before the identifier may be used to query data collected under section 702, for a foreign intelligence purpose, other than in exigent circumstances or where otherwise required by law."[72] It appears that this recommendation has not been implemented, so it likely will be discussed. It has an analog of sorts in the USA Freedom Act of 2015, which modified the prior program of bulk collection of telephony metadata in several ways, including by requiring the FISC's approval of selectors used for searches of providers' call detail records.[73] One possible compromise would be to require FISC approval only for queries of upstream data, which has the highest risk of involving unrelated US person communications, although that would be an expansion of existing upstream querying authority.

A related question concerns the FBI's ability to query un-minimized FAA § 702 data for evidence of a crime, particularly a crime not related to foreign intelligence.[74] The government reported in 2015 that "consistent with the recommendation of the Privacy and Civil Liberties Oversight Board, information acquired under section 702 about a US person will not be introduced as evidence against that person in any criminal proceeding except (1) with the approval of the Attorney General, and (2) in criminal cases with national security implications or certain other serious crimes. This change will ensure that, if the Department of Justice decides to use information

acquired under section 702 about a US person in a criminal case, it will do so only for national security purposes or in prosecuting the most serious crimes."[75] The FBI has reported that "it is extremely unlikely that an agent or analyst who is conducting an assessment of a non-national security crime would get a responsive result from the query against the section 702–acquired data."[76] Two PCLOB members stated that they were "unaware of any instance in which a database query in an investigation of a non-foreign intelligence crime resulted in a 'hit' on 702 information, much less a situation in which such information was used to further such an investigation or prosecution."[77] Recent reporting on ISIL recruits in Europe suggests this may not always be the case, however, so the issue may be worth exploring further.[78]

Underlying this debate is an interesting, although somewhat technical, question of whether querying should be seen as a separate, stand-alone Fourth Amendment event, such that it must satisfy constitutional requirements on its own, or whether it is instead best seen as part of the overall Fourth Amendment event described by the FAA, which includes but is not limited to acquisition, retention, querying, and dissemination of information. The former seems to have some support in the historical position of the government going back to the 1980s,[79] but the latter is at least arguably more consistent with more recent authority, particularly in the context of FAA § 702.[80] It seems unlikely that Congress will tackle this technical, constitutional question in a focused manner.

C. International Data Sharing

At least two issues of international data sharing may arise in connection with FAA renewal. First, especially in the wake of the November 2015 Paris attacks, there will probably be some members of Congress who push for more sharing of un-minimized data with foreign partners, including but perhaps not limited to Five Eyes (France is not part of the Five Eyes). Un-minimized downstream (PRISM) data collected by NSA under FAA § 702 is routinely shared with the CIA and FBI; the argument will be that it should likewise be routinely shared with British, Canadian, or other allied intelligence services, who may be able to identify foreign intelligence information that US analysts would miss and who can be trusted to apply court-approved minimization procedures after training by NSA or the Department of Justice (DOJ). Other members of Congress, however, will raise concerns about such sharing with foreign partners, particularly because it will include incidentally collected information about US persons. Under section 8 of NSA's 2014 standard FAA § 702 minimization procedures, the agency may share un-minimized information only for technical or linguistic assistance, subject to strict limits on analytic use by the foreign government.[81] Of course, deviations from the standard procedures, allowing for more sharing in particular cases or settings, may be permitted if proposed by the government and approved on a case-by-case basis by the FISA Court.

Second, we may see discussion of data-sharing between the United States and the European Union, including the Schrems decision striking down the Data Transfer Safe Harbor, which was premised in part on European dissatisfaction with the FAA and other US surveillance practices.[82] The Safe Harbor issue will probably be resolved before 2017; but if it is not, it will surely figure in the debates over renewal of the FAA. One interesting aspect of the Safe Harbor debates, and some related debates about cross-border data requests discussed in part 3, is the extent to which European surveillance practices may be brought to light. There is certainly an argument that European intelligence collection is conducted with far less oversight and far fewer restrictions than US collection, and it is quite clear that data is legally safest from US governmental snooping when stored here rather than abroad.[83]

D. Technical Issues and Compliance

A fourth issue that is likely to arise needs only brief mention, even though it could be significant to the legislative debates: NSA compliance problems. These problems have been well-documented in several areas and will likely be reviewed again in connection with FAA renewal. As the PCLOB noted, "[a] failure to implement the acquisition in a manner that reasonably limits the collection to the authorized purpose of the section 702 certifications can, and has, led to incidents of noncompliance with the minimization procedures that have been reported to the FISC and Congress."[84] As it ingests more and more data, the government will be more and more dependent on data-tagging at (or just after) acquisition, in order to effectuate subsequent controls governing access, use (e.g., querying), purge, and dissemination rules and requirements.[85]

The compliance regime will be even more complex to administer as the intelligence community continues work on its Integrated Intelligence Enterprise (IC-ITE)—referred to by the Office of the Director of National Intelligence (ODNI) as "the largest IT transformation in the history of the intelligence community"—which would create shared cloud-type servers for multiple agencies, each of which may have different access rights and requirements.[86] If the data-tagging efforts fail, the inter-agency compliance regime that rests atop it will likewise fail. Congress will likely want to explore this further in connection with FAA renewal because it is at the core of the government's ability to comply with minimization procedures and other limits, and also critical to its ability to limit access to information and mitigate the insider threat of further unauthorized disclosures.

E. Purpose of Collection

The FAA authorizes collection only when the government has at least a significant purpose to acquire "foreign intelligence information." That term is defined in two ways in the statute. The first part of the definition concerns what is typically referred to as

"protective" foreign intelligence, including information necessary or relevant to the ability of the United States to protect against attack, sabotage, espionage, international terrorism, or the proliferation of weapons of mass destruction by a foreign power. The second part defines "affirmative" foreign intelligence, including information concerning non-US persons that relates to the national defense or security of the United States or the conduct of the foreign affairs of the United States, but only insofar as that information concerns a foreign power or foreign territory.[87] The PCLOB reported that the FISC has approved certifications authorizing collection under section 702 for "categories of information" that satisfy the definition of foreign intelligence information, including "information concerning international terrorism and other topics, such as the acquisition of weapons of mass destruction." Particularly in light of PPD-28 and related statements from the Obama administration emphasizing the dignity and privacy interests of non-US persons, Congress can be expected to debate whether the FAA should continue to authorize collection of "affirmative" foreign intelligence as well as "protective" foreign intelligence.[88]

F. Executive Order 12333

As of this writing, the PCLOB is working on a report on surveillance under Executive Order 12333, the main presidential-level directive governing the US intelligence community.[89] Depending on the timing and nature of the report, legislative debate over FAA renewal will almost surely address surveillance under EO 12333. It seems all but inevitable that at least some members of the PCLOB will recommend a variety of measures designed to constrain EO 12333 surveillance and to make it more like surveillance under FAA § 702. Such changes might also include provisions akin to those in FAA § 702 authorizing compelled assistance from communications providers in connection with EO 12333 surveillance, although this might be opposed by US providers on the ground that it would exacerbate the perceived disparity between them and their foreign competitors in protecting privacy. Changes to the executive order in light of PPD-28 may also be called for by the PCLOB, because the two documents are significantly in tension with respect to their views concerning the privacy interests of non-US persons. It seems very probable that the Obama administration will support at least some of these measures; the next president's views are less certain. Perhaps the debate will go even further, and address whether Congress should enact comprehensive legislation governing all intelligence surveillance, or even charter statutes for all intelligence activities, as was considered in the 1970s.[90] Of all the issues reviewed here that might arise in connection with FAA renewal, this is the only one that I believe has the potential to result in really profound change to the status quo.

3. Longer-Term Predictions

Although I expect the FAA debate to unfold roughly as described above (absent a major disruption), it remains a very unsettled time for US national security in

general and foreign intelligence surveillance in particular. As discussed in part 1, the Snowden disclosures and the US government's reaction to those disclosures, coupled with increasing global instability and the rise of ISIL, have created a strange political environment both here and abroad. In that environment, the increasing and varied use of encryption, the growing fragmentation and indeterminacy of location in communications networks, communications providers' new reluctance to assist the government with surveillance requests, the expanding Internet of Things, and the explosion of open source and social media data all portend profound change. In this part of the paper, I describe these emerging political and technological developments and predict effects over the next several years. In general, the developments are presented in order, beginning with those I perceive as most likely to have the most significant, most identifiable impact in the nearest term.

A. Encryption and "Technical Assistance"

In the United States, at least, the November 2015 Paris attacks seemed to reopen a debate that previously had closed, concerning whether the government should enjoy "exceptional access" to encrypted communications and data so that it can effectuate surveillance directives.[91] There is a recent and well-developed literature on that topic,[92] addressing both technical and policy issues, and no need to reproduce it here. But there are two related points worth making, both of which directly concern FISA, the FAA, and foreign intelligence surveillance in general.

First, if present trends continue, in the absence of a new statute dealing expressly with encryption, there will be increasing pressure on the "technical assistance" requirements in FISA (and the Wiretap Act). Under several provisions of FISA, including the FAA, a telecommunications provider or other party may be directed to provide "technical assistance" (or simply "assistance") to the government in implementing the authorized activity. For example, a traditional FISA order for electronic surveillance "shall direct" that

> upon the request of the applicant, a specified communication or other common carrier, landlord, custodian, or other specified person . . . furnish the applicant forthwith all information, facilities, or technical assistance necessary to accomplish the electronic surveillance in such a manner as will protect its secrecy and produce a minimum of interference with the services that such carrier, landlord, custodian, or other person is providing that target of electronic surveillance.[93]

The FAA has similar language in two of its three main provisions, although it applies only to electronic communication service providers, not to custodians, landlords or other persons.[94] For section 702 surveillance, targeting non-US persons

reasonably believed to be abroad, the attorney general and the director of national intelligence (DNI)

> . . . may direct, in writing, an electronic communication service provider to . . . immediately provide the Government with all information, facilities, or assistance necessary to accomplish the acquisition in a manner that will protect the secrecy of the acquisition and produce a minimum of interference with the services that such electronic communication service provider is providing to the target of the acquisition.[95]

Indeed, section 702 surveillance may only be conducted with the assistance of a provider.[96] Compelled assistance is also part of FAA § 703, which governs targeting of US persons reasonably believed to be located abroad where the surveillance would otherwise require a traditional FISA court order and is conducted in the United States.[97] But there is no provision for compelled assistance in FAA § 704, which governs targeting of US persons abroad when the surveillance would not otherwise require an order and is conducted abroad: under section 704, the FISA Court does not even have "jurisdiction to review the means by which an acquisition under this section may be conducted," let alone issue an assistance order.[98] Section 704 is accomplished by the government acting alone, or with voluntary cooperation from others.

The Supreme Court addressed "technical assistance" in 1977 in US v. New York Tel. Co.,[99] where it held that the All Writs Act, which allows federal courts to "issue all writs necessary or appropriate in aid of their respective jurisdictions and agreeable to the usages and principles of law,"[100] could be used to compel a telephone company to assist with installation of a pen register. The pen register itself was authorized under Federal Rule of Criminal Procedure 41, but the court nonetheless noted the technical assistance provision in the Wiretap Act, explaining that in light of the act's "direct command to federal courts to compel, upon request, any assistance necessary to accomplish an electronic interception, it would be remarkable if Congress thought it beyond the power of the federal courts to exercise, where required, a discretionary authority to order telephone companies to assist in the installation and operation of pen registers, which accomplish a far lesser invasion of privacy."[101]

As encryption becomes more common, both in transmission and in devices, the government may seek more in the way of technical assistance from providers or others to defeat that encryption.[102] In the Eastern District of New York, the Department of Justice and Apple are at this writing engaged in a dispute about whether Apple can be compelled to unlock an iPhone for which there is a federal search warrant. The government is relying on the All Writs Act and New York Tel. Co., and Apple is claiming that the All Writs Act does not apply based on CALEA,[103] a 1994 statute that requires telecommunications providers to maintain their networks in certain ways that allow for

wiretapping but does not apply to stored data on a handset. Apple's main argument is that the All Writs Act cannot be used to compel what Congress declined to address in CALEA—i.e., that CALEA occupies the field of compelled assistance.[104]

There is very little publicly available law on the limits of "technical assistance" in FISA. A divided panel of the Ninth Circuit held that the Wiretap Act could not be used to compel assistance with a wiretap in ways that entirely disabled the communications system for the particular customer involved in the surveillance. The majority concluded that disabling the system was inconsistent with the statutory command that technical assistance be provided "in such a manner as will protect its secrecy and produce a minimum of interference with the services that such carrier . . . is providing that target of electronic surveillance":

> . . . the "a minimum of interference" requirement certainly allows for some level of interference with customers' service in the conducting of surveillance. We need not decide precisely how much interference is permitted. "A minimum of interference" at least precludes total incapacitation of a service while interception is in progress. Put another way, eavesdropping is not performed with "a minimum of interference" if a service is completely shut down as a result of the surveillance.[105]

The dissenting judge, Richard Tallman, concluded that the "minimum of interference" standard governed the manner in which technical assistance must be provided, not whether it must be provided. For Judge Tallman, it was enough that "the Company complied with the challenged order in the way least likely to interfere with its subscriber's services" and that "the only method of executing the intercept order in this case" was the one used, because "even the complete shutdown of a service [for a particular user] can represent the *minimum* interference, so long as no lesser amount of interference could satisfy the intercept order."[106] Judge Tallman's dissent is noteworthy, in part because he is a member of the Foreign Intelligence Surveillance Court of Review, with a term of service expiring in 2021.[107]

In general, the "technical assistance" requirement admits of a balancing of the provider's costs and burdens on the one hand against governmental need and alternatives on the other. It is therefore notable that in its case in New York, one of the burdens described by Apple is the following:

> . . . public sensitivity to issues regarding digital privacy and security is at an unprecedented level. This is true not only with respect to illegal hacking by criminals but also in the area of government access—both disclosed and covert. Apple has taken a leadership role in the protection of its customers' personal data against any form of improper access. Forcing Apple to extract data in this case, absent clear legal authority to do so, could threaten the trust between Apple and its customers and substantially tarnish the Apple brand. This

> reputational harm could have a longer term economic impact beyond the mere cost of performing the single extraction at issue.[108]

Taken to its logical conclusion, this might mean that a provider could create its own undue burden by strongly and publicly opposing assistance with governmental surveillance.

A second issue concerns the difference between providing technical assistance and configuring communications networks to facilitate surveillance. As discussed above, the former is required by FISA and the Wiretap Act, while the latter is required in limited circumstances by CALEA. Absent an amendment to any of these laws, there will be at least two critical questions where CALEA by its terms does not apply. First, as a legal matter, what is the distinction between configuring "equipment, facilities, or services" under CALEA and providing "technical assistance" under FISA and the Wiretap Act? For example, is it "technical assistance" for a provider to push down to a user's phone, with or perhaps without the user's knowledge, a software patch or program that facilitates surveillance (e.g., by covertly disabling encryption)? Does the answer change if the software (code) is written by the government rather than the provider itself? These issues may matter more today than they did in the era in which the Wiretap Act, FISA, and CALEA were enacted, because in at least some settings, software has become more important than hardware for facilitating surveillance. Second, to what extent can uncooperative providers configure their "equipment, facilities, or services" to thwart surveillance without depriving themselves of functionality desired by themselves or their customers? For example, will providers be willing to eschew any capacity to add an invisible third party to communications on their networks? If not, the capacity may be available as technical assistance for governmental surveillance. There is enough uncertainty on these issues that Congress may want to consider some clarification.

Other countries are tackling the issue now. In the United Kingdom, for example, the November 2015 draft of a new Investigatory Powers Act is quite explicit. It deals directly with what the British call "equipment interference," which "allows the security and intelligence agencies, law enforcement and the armed forces to interfere with electronic equipment such as computers and smartphones in order to obtain data, such as communications from a device." Equipment interference "encompasses a wide range of activity from remote access to computers to downloading covertly the contents of a mobile phone during a search." It is necessary to avoid "the loss of intelligence that may no longer be obtained through other techniques, such as interception, as a result of sophisticated encryption."[109]

In case the UK bill is not clear enough on its face, the Electronic Frontier Foundation (EFF) asserts in public comments on the bill that the "common term for 'equipment interference' is 'hacking': breaking into and remotely controlling devices. It permits third

parties to transform a general-purpose device such as a modern smartphone, laptop, or desktop computer into a surveillance machine."[110] Although the term "'equipment interference' carries with it the implication that the power is restricted to impeding normal equipment operations," EFF asserts, it "may also include adding unexpected new functionality to a device," such as surveillance functionality.[111] The EFF comments further argue that under the UK's bill, third parties can be compelled to assist in hacking: "a warrant might be served on British Telecom, for example, to compel them to interfere with a device they neither own nor legally control, such as a phone using their network in order to access its voicemail."[112] Indeed, EFF asserts, "[u]nder the proposed law, a British company could be compelled to distribute a [software] update in order to facilitate the execution of an equipment interference warrant and ordered to refrain from notifying their customers . . . Such an update could be targeted at an individual, an organisation, or many organisations related to a single investigation."[113] The draft IP bill also authorizes bulk collection and (in certain circumstances) equipment interference in bulk.[114] Whether or not the EFF comments are completely accurate in their characterization of the UK bill, they clearly illustrate the range of issues and conduct that might be authorized or prohibited by new surveillance laws.

It would be worthwhile for Congress to consider the limits of "technical assistance" in the context of equipment interference and other techniques that might be used to defeat at least some forms of encryption. This would include legal issues as well as technical ones, depending on whether the interference action is to be accomplished by the government or the provider, and of course the relevant policy questions.

B. Provider Cooperation

Ironically, the government's increasing reliance on "technical assistance" from providers will occur at a time when US providers are less inclined than they once were to cooperate with surveillance requests.[115] American law, however, still assumes that providers will cooperate, at least in some cases, even when not required to do so. Coupled with the increasing storage of data abroad,[116] this creates at least two significant surveillance gaps that Congress should examine.

First, whatever the merits of Microsoft's argument in the case of the drug dealer discussed above (part 1), there is no real doubt that it would prevail if the government sought e-mail stored in Ireland under traditional FISA. That is because traditional FISA searches may only occur in the United States, and traditional FISA electronic surveillance applies to stored data only when the surveillance device is used in the United States.[117] Indeed, this was part of the assessment underlying the decision by Congress to enact the FAA in 2008.[118] When it comes to US persons, however, the FAA is no help in reaching e-mail stored abroad. As discussed above, section 702 does not apply to US persons; section 703 applies only when the surveillance is conducted

in the United States; and section 704 has no "technical assistance" or compelled production provisions at all. In short, unless the provider voluntarily repatriates the US person's stored e-mail, its production cannot be compelled under FISA.

The same is true if the target of the surveillance or search is a non-US person located in the United States: his e-mail in Ireland is beyond the reach of traditional FISA, as discussed above, and his location in this country puts him outside the reach of FAA § 702. In sum, then, when e-mail is stored abroad, neither traditional FISA nor the FAA can be used to compel provider assistance if the target is either a US person (in any location) or a person (of any nationality) located in the United States. This is a potentially significant shortfall in FISA, particularly as data become more and more mobile, subject to being stored in any location, or even fragmented and stored in several locations at once.

A second possible gap concerns the situation in which all parties to a phone call or e-mail are located abroad, but the communication transits a wire in the United States. In that situation, it has long been the case that the US government generally cannot get a FISA Court order to compel the assistance of the provider that owns the wire.[119] Unless it has a valid target under FAA § 702—i.e., a non-US person located abroad—the most the government can do is assure the provider, in the form of a certification from the attorney general, that it *may* lawfully cooperate, but not that it *must* do so.[120] If a provider refuses, the government has very little recourse. Today, with providers more recalcitrant than they have been, based on their public statements, voluntary assistance may not be forthcoming.

Congress should consider these questions. Some observers will instinctively approve of any change that reduces collection opportunities, while others will instinctively disapprove. But Congress should approach the matter more systematically. The alternative is effectively to delegate authority to the communications providers, who are focused on profit and other fiduciary duties to their shareholders, rather than the public interest, and who are reacting to events largely controlled by others with no accountability to US voters.

C. Cross-Border Data Requests

As Europe expands surveillance authorities and the United States contracts, and as encryption proliferates in ways that challenge surveillance without providers' technical assistance, there will be more focus on cross-border data requests—i.e., situations in which a government tries to compel the production of data located outside its national borders. Today, major US providers face escalating pressure from European governments, asserting their own laws to require production of data stored by the providers in the United States, in ways that violate US law. At the same time, foreign governments

also are increasingly likely to enact laws forbidding production of locally held data in response to US (and other) demands for its production, and also to enact laws requiring certain data to be held locally, creating a form of reciprocal pressure. International agreements could help reduce this dissonance and also rationalize surveillance rules to promote international commerce, law enforcement, protection of civil liberties, and the worldwide rule of law. Developing such international agreements will be challenging, but the alternative is an increasingly chaotic and dysfunctional system for cross-border data requests that benefits no one. There has been a good deal of recent scholarship on this topic, and Congress should be sure to address it soon.[121]

D. Location

As discussed above, cheap, user-friendly data encryption seems to have reached, or nearly reached, a tipping point, where it becomes the default instead of an esoteric option for communications and stored data. Not far behind may be location-spoofing, through technologies such as virtual private networks (VPNs). Of course, the government has been dealing with anonymity and location spoofing for some time due to TOR.[122] But VPNs may be more significant because, among other things, they are more user-friendly and might be more widely adopted. Companies offering VPN service create an encrypted connection between the user's device and their own servers, and allow the user to connect to the Internet from those servers. In doing so, the user's apparent IP address corresponds to the VPN server, which may or may not be in the same country as the user. Ordinary persons may use VPNs to protect their privacy or their personal data from cybercrime, or perhaps to defeat geo-blocking, a location-based limit on access to content on the Internet that relies on IP addresses to filter eligible users.[123] But VPNs or other technology that spoofs location to defeat geo-blocking filters could also raise problems for administration of FAA § 702. As discussed above, section 702 permits surveillance only when the government has a reasonable belief that the target is abroad, and NSA uses IP address as a means of determining location.[124] Coupled with the continued growth of mobile communications at the expense of fixed-point communications, and the increasing number of people who do in fact roam across national borders, the widespread adoption of location-spoofing technology could create real problems.

It appears that ISIL has provided guidance to its members and affiliates on the use of encryption;[125] if it has not already done so, ISIL also could provide guidance on the use of TOR, VPNs or similar services, or users could consult the Internet directly for instructions. To be sure, NSA almost surely has other technical or human methods at its disposal to help determine location, and it may also have lists of IP addresses associated with known VPN providers that it might be able to persuade the FISA Court to ignore as evidence of location in the court-approved targeting procedures or otherwise. But NSA's current approach requires analysts to get to the bottom of conflicting information

about a target's location, rather than adopting a simple more-likely-than-not mechanical test. What this means, in practical terms, is not only that conflicts must be resolved before targeting can occur, but also that the emergence of new information about an existing target may require immediate attention and de-tasking if the discrepancy cannot be resolved. As the PCLOB explained in its report on FAA § 702:

> Commentators have questioned the rigor of the agency's "foreignness" determinations, particularly whether they rely on certain default assumptions where information about a person is lacking. The notion also has arisen that the agency employs a "51 percent test" in assessing the location and nationality of a potential target—in other words, that analysts need only be slightly more than half confident that the person being targeted is a non-US person located outside the United States.
>
> These characterizations are not accurate. In keeping with representations the government has made to the FISA court, NSA analysts consult multiple sources of information in attempting to determine a proposed target's foreignness; they are obligated to exercise a standard of due diligence in that effort, making their determinations based on the totality of the circumstances. They also must document the information on which they based their assessments, which must be reviewed and approved by two senior analysts prior to targeting and which are subject to further review later.[126]
>
> With respect to the foreignness determination, the NSA analyst is required to assess whether the target of the acquisition is a non-US person reasonably believed to be located outside the United States based upon the totality of the circumstances available. This analysis begins with a review of the initial lead information, which must be examined to determine whether it indicates either the location or the US person status of the potential target. At times, the lead information itself will state where the target is assessed to be located and their US person status. In other instances, this information may only enable an analyst to infer location or US person status. In either case, the section 702 targeting determination may not be made upon the lead information alone. Instead, the NSA analyst must check multiple sources and make a determination based on the totality of the circumstances available to the analyst.
>
> The government has stated that in making this foreignness determination, the NSA targeting procedures inherently impose a requirement that analysts conduct "due diligence" in identifying these relevant circumstances. What constitutes due diligence will vary depending on the target; tasking a new selector used by a foreign intelligence target with whom the NSA is already quite familiar may not require deep research into the target's (already known) US person status and current location, while a great deal more effort may be required to target a previously unknown, and more elusive, individual. As previously discussed above, a failure by an NSA analyst to conduct due diligence in

> identifying relevant circumstances regarding the location and US person status of a section 702 target is a reportable compliance incident to the FISC.
>
> After conducting due diligence and reviewing the totality of the circumstances, the NSA analyst is required to determine whether the information indicates that the target is a non-US person reasonably believed to be located outside the United States. The government has stated, and the Board's review has confirmed, that this is not a "51 percent to 49 percent test." If there is conflicting information indicating whether a target is located in the United States or is a US person, that conflict must be resolved and the user must be determined to be a non-US person reasonably believed to be located outside the United States prior to targeting.[127]

In sum, as NSA's director of civil liberties and privacy has explained, "[i]f the analyst discovers any information indicating the targeted person may be located in the US or that the target may be a US person, such information must be considered. In other words, if there is conflicting information about the location of the person or the status of the person as a non-US person, that conflict must be resolved before targeting can occur."[128] Given this requirement to resolve conflicting information about a target's location, and the scale of FAA § 702 collection (probably around 100,000 targets), location-spoofing does not need to work 100 percent of the time, or even 20 percent of the time, to create significant administrative problems, delay, and uncertainty in the application of the law and repeated de-tasking and re-tasking of selectors.

It may be that NSA's tools are so sophisticated that even a concerted effort by ISIL or others to spoof IP addresses would have negligible impact.[129] But Congress should satisfy itself that this is the case in connection with FAA renewal, because if it is not, the statute might require a *major* overhaul. To the extent that the true locations of users of targeted selectors cannot be determined consistently, reliably, and quickly, the FAA is to that extent in deep trouble. It is not clear to me that we have the technical expertise, conceptual models, and political consensus necessary to write and enact a next generation of surveillance laws that balance privacy and security effectively and constitutionally.[130]

Even in the absence of intentional efforts to spoof location, increasing fragmentation of the Internet will also pressure the role of location in surveillance law. Compared to just a few years ago, global communications networks are much bigger and faster, and are likely to continue growing, whether measured by the number of users, number of web pages, or amount of data available and transmitted.[131] At the same time, transmission facilities are proliferating, with more and more undersea cables being laid and planned[132] and fewer chokepoints for transiting communications of all kinds. For example, Brazil is planning for an undersea cable connecting South America directly to

Europe, without transiting the United States, apparently motivated in part by desires to avoid US surveillance[133] (although such surveillance has been publicly known since at least the 1970s).[134]

One result, not readily amenable to legal solution, is that the US home field advantage in surveillance is receding. By one estimate, before 2001, 80 percent of the world's communications traffic transited the United States, while now it is less than 20 percent (albeit of a much higher total number of communications).[135] This estimate may or may not be numerically accurate, but the trend is unmistakable. On the other hand, the increase in the total amount of data also creates problems in the form of ever-larger haystacks in which the government must find the needles.[136]

Another result of increasing fragmentation may be that there are fewer communications facilities dedicated to carrying international rather than domestic traffic, meaning that packets from domestic and international communications may increasingly be found in the same locations. That seems to be part of what has challenged NSA's "upstream" collection, as discussed above. To the extent that is the case, however, it challenges another aspect of FISA's basic regulatory approach: the distinctions based on where data is acquired, which were premised on the view that acquisition domestically deserved more protection because of the higher incidence of domestic communications.[137] That is still probably true, for at least some domestic facilities, to a great extent, but it is becoming less true over time. For the long run, Congress may want to reconsider distinctions between surveillance conducted in the United States and surveillance conducted abroad.

E. Internet of Things and FinTech

It is commonplace today to acknowledge the expanding Internet of Things (IOT), in which devices ranging from toasters to air conditioners to door locks are connected to the Internet and to each other,[138] and fintech, which involves the intersection of finance and technology.[139] There are many interesting business issues raised by the IOT and fintech, and some very interesting operational issues relevant to national security (such as the availability and durability of what may be a host of new network access points for surveillance, and vulnerabilities for hacking, and new communications capabilities embedded in financial transactions).[140] There are also several legal issues related to national security and surveillance. For example, the profusion of connected devices and data types will challenge existing collection paradigms, and perhaps the distinction between contents and metadata.[141] The profusion of new "providers" may challenge existing definitions in FISA and the FAA, both as to who may be compelled to provide technical assistance and the nature of that assistance, and will certainly pose cultural challenges—e.g., if and when a manufacturer of Internet-connected door locks receives its first FISA order as part of an authorized physical search.[142]

F. Expanded Open Source Data, Social Media, and the Cloud

Finally, over time the government will need to address a series of issues arising from the increasing number of digital footprints left by almost all users of the Internet, especially users of social media. Among the issues are the following. First is the question of governmental access to this data. One perspective is that if the data are freely available on the Internet, the government also should be able to review them. A competing perspective, of course, is that the government should not be reviewing my Facebook posts without meeting some standard of suspicion. Second, of course, not all open source data is freely available to everyone—some data may require elicitation by a government agent or an agent's undisclosed participation in a forum such as an online chat room. Is data "open source" if a government agent needs to create a false online identity (or otherwise violate a provider's terms of service) to access it? Is it open source if the agent uses her real online identity (and doesn't violate the terms of service)? Third, there is the question of possible bulk collection of open source data—e.g., how would Americans feel about NSA ingesting public data on all real estate transactions from Dearborn, Michigan, and then querying it selectively over time? To be sure, there are guidelines that govern access to open source data, such as the FBI's Domestic Investigations and Operations Guide (DIOG), DOD 5240.1-R, and DOD-I 3115.12, and an inter-agency National Open Source Committee (NOSC) to consider policy issues.[143] But it is not clear that the guidelines have kept up with recent changes. Fourth, the increasing use of social media for terrorist propaganda only complicates matters and introduces First Amendment issues as well.[144]

There is also a series of questions from the perspective of counter-intelligence. For example, there have been concerns about the security of privately held open source data. In other words, could Facebook be the next Office of Personnel Management?[145] Although Internet and cloud providers may have better security than most individual users, they are obviously attractive targets for hackers because they hold so much data. For example, Google revealed in 2011 that "unknown hackers likely originating from central China tried to hack into the Gmail accounts of hundreds of users, including senior US government officials, Chinese activists and journalists."[146] The director of the CIA's personal e-mail account was hacked in 2015.[147] Today, with entire digital personae available online, will terrorists and spies need to jettison their identities the way they used to dispose of mobile telephones? Will future undercover agents or NOC operatives need to do so? And if they take steps to avoid using the Internet during a period of classified training, will that gap immediately expose them as government agents? These and many related questions remain to be addressed by policymakers.

4. Conclusion

There is a significant contrast between the two analytical parts of this paper. With the possible exception of modifications to Executive Order 12333, most of the issues

discussed in part 2 are interstitial and fit within our existing paradigms. Whether to permit US person queries of upstream data, for example, is an important question, but one on which reasonably educated policymakers can make a choice without fear of truly revolutionary effects. The issues discussed in part 2 will be most significant when the solutions are considered in the aggregate, rather than individually. Death by a thousand cuts—considered from the perspective of privacy or security—is the concern here.

The issues in part 3 of the paper, by contrast, strike me as substantially more significant, and difficult. For example, if the government cannot use FISA to compel access to stored e-mail of non-US persons located in the United States, it is a big deal; if encryption makes all Western governments more reliant on provider technical assistance and providers continue to resist, and if cross-border data requests can't be dealt with efficiently, it is a very big deal; and if the basic location-based grammar of the FAA fails because of increased location-spoofing or other developments, it is a huge deal. Debates over renewal of the FAA in the next two years will very likely include the issues set out in part 2 of this paper. I hope they will also include some of the issues set out in part 3, or that Congress and the executive branch will consider them carefully in a separate process.[148]

NOTES

1 The Privacy and Civil Liberties Oversight Board (PCLOB) describes itself as follows:

> The PCLOB is an independent agency within the executive branch established by the Implementing Recommendations of the 9/11 Commission Act of 2007. The bipartisan, five-member Board is appointed by the President and confirmed by the Senate. By statute, the Chairman serves full time, but the four other Board members serve in their positions part-time. The PCLOB's mission is to ensure that the federal government's efforts to prevent terrorism are balanced with the need to protect privacy and civil liberties.

About the Board, Privacy and Civil Liberties Oversight Bd., https://www.pclob.gov/about-us.html.

In July 2014, the PCLOB released a report on the FAA: Privacy and Civil Liberties Oversight Board, *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act* (2014) [hereinafter *PCLOB 702 Report*], https://www.pclob.gov/library/702-Report.pdf.

2 The FISA Amendments Act of 2008, Pub. L. No. 110-261, 122 Stat. 2436 (2008), is scheduled to sunset on December 31, 2017. *See* FISA Amendments Act Reauthorization Act of 2012, Pub. L. No. 112-238, 126 Stat. 1631 (2012); Clapper v. Amnesty Intern. USA, 133 S. Ct. 1138, 1144 n.2 (2013). For a detailed discussion of the FAA, including events leading up to its enactment, an analysis of its political, legal and technological aspects, and a description of how it functions, including its exclusivity provisions, *see* David S. Kris & J. Douglas Wilson, *National Security Investigations and Prosecutions,* chs. 15–17 (2d ed. 2012) [hereinafter NSIP].

3 The FAA also increased protections for US persons located abroad. For a more complete discussion of the FAA, *see* NSIP, *supra* note 2, at chs. 16–17.

4 Office of the Dir. of Nat'l Intelligence, *Statistical Transparency Report Regarding Use of National Security Authorities—Annual Statistics for Calendar Year 2014* (Apr. 22, 2015), http://icontherecord.tumblr.com/transparency/odni_transparencyreport_cy2014; Office of the Dir. of Nat'l Intelligence, *Statistical Transparency Report Regarding Use of National Security Authorities—Annual Statistics for Calendar Year 2013* (June 26, 2014), http://icontherecord.tumblr.com/transparency/odni_transparencyreport_cy2013.

5 For a discussion of these debates, *see, e.g.*, NSIP, *supra* note 2, § 19:4.50 (Supp. 2015).

6 President Barack Obama, Remarks by the President at the National Defense University (May 23, 2013), https://www.whitehouse.gov/the-press-office/2013/05/23/remarks-president-national-defense-university. The president summarized his conclusions about terrorism as follows:

> So that's the current threat—lethal yet less capable al Qaeda affiliates; threats to diplomatic facilities and businesses abroad; homegrown extremists. This is the future of terrorism. We have to take these threats seriously, and do all that we can to confront them. But as we shape our response, we have to recognize that the scale of this threat closely resembles the types of attacks we faced before 9/11.
>
> In the 1980s, we lost Americans to terrorism at our embassy in Beirut; at our Marine barracks in Lebanon; on a cruise ship at sea; at a disco in Berlin; and on a Pan Am flight—Flight 103—over Lockerbie. In the 1990s, we lost Americans to terrorism at the World Trade Center; at our military facilities in Saudi Arabia; and at our embassy in Kenya. These attacks were all brutal; they were all deadly; and we learned that left unchecked, these threats can grow. But if dealt with smartly and proportionally, these threats need not rise to the level that we saw on the eve of 9/11.

DOJ revised its media investigation guidelines in January 2014. *See* Kevin Johnson, *DOJ Issues New Guidelines for Dealing with Media,* USA Today (Jan. 14, 2014), http://www.usatoday.com/story/news/nation/2015/01/14/doj-guidelines-media/21754099 ("The Justice Department on Wednesday put additional limitations on federal prosecutors investigating leaks of classified material in cases that involve the pursuit of information gathered by journalists.")

7 President Barack Obama and President Macky Sall, Remarks by President Obama and President Sall of the Republic of Senegal at Joint Press Conference (June 27, 2013), https://www.whitehouse.gov/the-press-office/2013/06/27/remarks-president-obama-and-president-sall-republic-senegal-joint-press-. These remarks were widely understood as an effort to "downplay" the significance of Snowden. *See, e.g.*, Nancy Benac, *Obama Recasts Edward Snowden As 'Hacker' In Effort To Downplay Him,* Huffington Post (June 28, 2013), http://www.huffingtonpost.com/2013/06/28/obama-edward-snowden-hacker_n_3515562.html; Julie Pace, *Obama: No Wheeling or Dealing to Extradite Snowden,* Associated Press (June 27, 2013), http://news.yahoo.com/obama-no-wheeling-dealing-extradite-142135715.html.

8 The president made two references to surveillance in his May 2013 speech. First, in describing the aftermath of the 9/11 attacks, before he took office, he said: "And so our nation went to war. We have now been at war for well over a decade. . . . Meanwhile, we strengthened our defenses. . . . Most of these changes were sound. . . . But some, like expanded surveillance, raised difficult questions about the balance that we strike between our interests in security and our values of privacy." Later in the speech, the president said:

> Thwarting homegrown plots presents particular challenges in part because of our proud commitment to civil liberties for all who call America home. That's why, in the years to come, we will have to keep working hard to strike the appropriate balance between our need for security and preserving those freedoms that make us who we are. That means reviewing the authorities of law enforcement, so we can intercept new types of communication, but also build in privacy protections to prevent abuse.
>
> That means that—even after Boston—we do not deport someone or throw somebody in prison in the absence of evidence. That means putting careful constraints on the tools the government uses

> to protect sensitive information, such as the state secrets doctrine. And that means finally having a strong Privacy and Civil Liberties Board to review those issues where our counterterrorism efforts and our values may come into tension.

Remarks by the President at the National Defense University, *supra* note 6.

9 All of the quotations in this paragraph are from President Barack Obama, Remarks by the President in a Press Conference (Aug. 9, 2013), https://www.whitehouse.gov/the-press-office/2013/08/09/remarks-president-press-conference.

10 Brad Smith, *Unfinished Business on Government Surveillance Reform,* The Official Microsoft Blog (June 4, 2014), http://blogs.microsoft.com/on-the-issues/2014/06/04/unfinished-business-on-government-surveillance-reform. Smith is currently the president and chief legal officer of Microsoft. *See* Paul Barbagallo, *Microsoft Appoints General Counsel Brad Smith as President,* Bloomberg Business (Sept. 11, 2015), http://www.bloomberg.com/news/articles/2015-09-11/microsoft-appoints-brad-smith-as-president-chief-legal-officer. Other companies were also pushing for reforms. *See, e.g.*, Ellen Nakashima, *Tech Giants Don't Want Obama to Give Police Access to Encrypted Phone Data,* Wash. Post (May 19, 2015), http://www.huffingtonpost.com/2015/05/19/tech-giants-dont-want-oba_n_7336642.html. Susan Molinari, *Congress Has Only A Few Weeks Left to Modernize Surveillance Laws,* Google Pub. Pol'y Blog (April 29, 2015), http://googlepublicpolicy.blogspot.com/2015/04/congress-has-only-few-weeks-left-to_29.html; *USA FREEDOM Act: Time for Meaningful Government Surveillance Reform,* Yahoo: Global Pub. Pol'y (April 28, 2015), http://yahoopolicy.tumblr.com/post/117638169643/usa-freedom-act-time-for-meaningful-government.

11 Smith, *supra* note 10.

12 *See* Brief for Appellant at 10–12, *In re Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corporation,* No. 14-2985-cv (2d Cir. Aug. 12, 2014), https://www.eff.org/document/microsofts-second-circuit-opening-brief.

13 *See In re Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corporation,* 15 F. Supp. 3d 466 (S.D.N.Y. 2014) (*appeal pending*).

14 *See* Brief for Appellant at 1–2, *In re Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corporation,* No. 14-2985-cv (2d Cir. Aug. 12, 2014), https://www.eff.org/document/microsofts-second-circuit-opening-brief. The Introduction to the brief begins as follows:

> Imagine this scenario. Officers of the local Stadtpolizei investigating a suspected leak to the press descend on Deutsche Bank headquarters in Frankfurt, Germany. They serve a warrant to seize a bundle of private letters that a New York Times reporter is storing in a safe deposit box at a Deutsche Bank USA branch in Manhattan. The bank complies by ordering the New York branch manager to open the reporter's box with a master key, rummage through it, and fax the private letters to the Stadtpolizei.
>
> The U.S. Secretary of State fumes: "We are outraged by the decision to bypass existing formal procedures that the European Union and the United States have agreed on for bilateral cooperation, and to embark instead on extraterritorial law enforcement activity on American soil in violation of international law and our own privacy laws." Germany's Foreign Minister responds: "We did not conduct an extraterritorial search—in fact we didn't search anything at all. No German officer ever set foot in the United States. The Stadtpolizei merely ordered a German company to produce its own business records, which were in its own possession, custody, and control. The American reporter's privacy interests were fully protected, because the Stadtpolizei secured a warrant from a neutral magistrate."

> No way would that response satisfy the U.S. Government. The letters the reporter placed in a safe deposit box in Manhattan are her private correspondence, not the bank's business records. The seizure of that private correspondence pursuant to a warrant is a law enforcement seizure by a foreign government, executed in the United States, even if it is effected by a private party whom the government has conscripted to act on its behalf.
>
> This case presents a digital version of the same scenario, but the shoe is on the other foot.

Microsoft's position was somewhat challenged when the government of Ireland filed a brief conceding that it is "incumbent upon Ireland to acknowledge" that its own Supreme Court has "held that . . . there may be circumstances in which an Irish court would order the production of records from an Irish entity on foreign soil," perhaps even if "execution of the order would violate the law of the foreign sovereign." Brief of Amicus Curiae Ireland at 5–6, *In re Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corporation,* No. 14-2985-cv (2d Cir. Dec. 23, 2014) (italics in original) (citing *Walsh v. National Irish Bank* [2013] 1ESC 2), http://digitalconstitution.com/wp-content/uploads/2014/12/Ireland-Amicus-Brief.pdf.

15 Lisa Monaco, *Obama Administration: Surveillance Policies Under Review,* USA Today (Oct. 24, 2013), http://www.usatoday.com/story/opinion/2013/10/24/nsa-foreign-leaders-president-obama-lisa-monaco-editorials-debates/3183331.

16 Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act of 2015, Pub. L. No. 114-23, 129 Stat. 268 (USA FREEDOM Act). The amicus provisions of the Freedom Act are codified at 50 U.S.C. § 1803(i), and the provisions ending bulk collection are codified at 50 U.S.C. § 1861(b)(2)(C).

17 For a more complete discussion of the president's speech and PPD-28, *see* NSIP, *supra* note 2, § 19:4.50 (Supp. 2015).

18 For example, in a February 2015 release, ODNI described some of the ways in which the intelligence community has implemented PPD-28, noting that the directive "reinforces current practices, establishes new principles, and strengthens oversight, to ensure that in conducting signals intelligence (SIGINT) activities, the United States takes into account not only the security needs of our nation and our allies, but also the privacy of people around the world." Office of the Dir. of Nat'l Intelligence, *Signals Intelligence Reform 2015 Anniversary Report* (2015), http://icontherecord.tumblr.com/ppd-28/2015/privacy-civil-liberties. In the same document, the DNI described himself as being "pleased to report that, as required by PPD-28, all Intelligence Community elements have reviewed and updated their existing policies and procedures, or have issued new policies or procedures, to provide safeguards for personal information collected through SIGINT, regardless of nationality and consistent with national security, our technical capabilities, and operational needs." For a more complete discussion of PPD-28, *see* NSIP, *supra* note 2, § 19:4.50 (Supp. 2015).

19 Peter Swire, *US Surveillance Law, Safe Harbor, and Reforms Since 2013* (Dec. 17, 2015), https://fpf.org/wp-content/uploads/2015/12/White-Paper-Swire-US-EU-Surveillance.pdf.

20 *See* Ellen Nakashima and Andrea Peterson, *Obama Administration Opts Not to Force Firms to Decrypt Data—For Now,* Wash. Post (Oct. 8, 2015), https://www.washingtonpost.com/world/national-security/obama-administration-opts-not-to-force-firms-to-decrypt-data--for-now/2015/10/08/1d6a6012-6dca-11e5-aa5b-f78a98956699_story.html. By contrast, some of the 2016 presidential contenders, such as Hillary Clinton, are keeping options open on encryption and urging providers and the government to work together to find solutions. *See* Hillary Clinton on National Security and the Islamic State, Council on Foreign Rel. (Nov. 19, 2015), http://www.cfr.org/radicalization-and-extremism/hillary-clinton-national-security-islamic-state/p37266. In her CFR speech, Clinton said:

> Another challenge is how to strike the right balance of protecting privacy and security. Encryption of mobile communications presents a particularly tough problem. We should take the

> concerns of law enforcement and counterterrorism professionals seriously. They have warned that impenetrable encryption may prevent them from accessing terrorist communications and preventing a future attack. On the other hand, we know there are legitimate concerns about government intrusion, network security, and creating new vulnerabilities that bad actors can and would exploit. So we need Silicon Valley not to view government as its adversary. We need to challenge our best minds in the private sector to work with our best minds in the public sector to develop solutions that will both keep us safe and protect our privacy. Now is the time to solve this problem, not after the next attack.

In a speech at the University of Minnesota in mid-December 2015, Clinton said this:

> Now, encryption of mobile devices and communications does present a particularly tough problem with important implications for security and civil liberties. Law enforcement and counterterrorism professionals warn that impenetrable encryption may make it harder for them to investigate plots and prevent future attacks. On the other hand, there are very legitimate worries about privacy, network security, and creating new vulnerabilities that bad actors can exploit.
>
> I know there's no magic fix to this dilemma that will satisfy all these concerns. But we can't just throw up our hands. The tech community and the government have to stop seeing each other as adversaries and start working together to keep us safe from terrorists. And even as we make sure law enforcement officials get the tools they need to prevent attacks, it's essential that we also make sure jihadists don't get the tools they need to carry out attacks.

Hillary Clinton Lays Out Comprehensive Plan to Bolster Homeland Security (Dec. 15, 2015), https://www.hillaryclinton.com/briefing/statements/2015/12/15/comprehensive-plan-to-bolster-homeland-security.

21 Of course, some observers presumably believe the Obama administration did not go far enough in advancing reforms, while others may believe it went too far. An interesting question, which may be answered during calendar year 2016, is the extent to which the US intelligence community will depart, in public or in private, from the Obama administration's official positions on national security issues. There are certainly at least pockets of resentment against the administration within the community, and serious disagreement with some of its policies. *See, e.g.*, Adam Entous & Danny Yadron, *Some Senior U.S. Officials Not Comfortable with Obama's Curbs on NSA Spying on Leaders,* Wall Street Journal (Dec. 30, 2015), http://www.wsj.com/articles/some-senior-u-s-officials-not-comfortable-with-obamas-curbs-on-nsa-spying-on-leaders-1451506801. With respect to encryption, for example, FBI Director Comey called publicly for legislation to address the issue in 2014, and then, after the administration decided not to seek such legislation, the FBI in 2015 apparently continued to meet with congressional staff about the topic. *See* James Comey, Keynote Address at Going Dark: Are Technology, Privacy and Public Safety on a Collision Course?, Brookings Inst. (Oct. 16, 2014) (transcript available at http://www.brookings.edu/~/media/events/2014/10/16%20going%20dark%20technology%20privacy%20comey%20fbi/20141016_fbi_comey_transcript.pdf) at 14; David Perera, *Terror Fears Don't Budge Obama on Encryption,* Politico (Dec. 17, 2015), http://www.politico.com/story/2015/12/obama-resists-calls-for-encryption-shift-216920 ("After warning in 2014 that encryption was hamstringing the FBI, Comey launched a yearlong campaign to persuade Congress to act. Even after being warned off earlier this year by the White House, FBI officials continued meeting with lawmakers and congressional staffers.").

22 *See, e.g.*, Press Release, Am. C.L. Union, ACLU & Tea Party Patriots Co-Sponsor TV Ads Calling for Washington to Rein In Government Surveillance (May 19, 2015), https://www.aclu.org/news/aclu-tea-party-patriots-co-sponsor-tv-ads-calling-washington-rein-government-surveillance.

23 Tom Cohen, *5 Years Later, Here's How the Tea Party Changed Politics,* CNN (Feb. 28, 2014), http://www.cnn.com/2014/02/27/politics/tea-party-greatest-hits/index.html.

24 *See, e.g.*, John Lapinski, Hannah Hartig & Stephanie Psyllos, *Poll: Donald Trump Still Leads GOP Field,* NBC News (Jan. 5, 2016), http://www.nbcnews.com/politics/2016-election/poll-donald-trump-still-leads-gop-field-n490116; Jessica Schulberg, *Rand Paul Ends Daylong NSA Filibuster*, Huffington Post (May 20, 2015), http://www.huffingtonpost.com/2015/05/20/rand-paul-nsa-filibuster_n_7347722.html.

25 *See* Dan Roberts, *Ted Cruz Rejects Demands to Revive NSA Surveillance after San Bernardino,* The Guardian (Dec. 10, 2015), http://www.theguardian.com/us-news/2015/dec/10/ted-cruz-nsa-surveillance-san-bernardino.

26 *See* Nick Gass, *After San Bernardino Massacre, Rubio Hits Cruz for Surveillance Vote,* Politico (Dec. 4, 2015), http://www.politico.com/story/2015/12/marco-rubio-ted-cruz-surveillance-vote-216428 ("In the wake of Wednesday's massacre in San Bernardino, California, Florida Sen. Marco Rubio on Friday dinged Ted Cruz and his other fellow senators and GOP presidential rivals for their votes to end the National Security Agency's bulk collection of phone metadata."); Joel Aschbrenner, *Christie Calls Out Cruz, Paul on Surveillance,* Des Moines Reg. (Dec. 4, 2015), http://www.desmoinesregister.com/story/news/elections/presidential/caucus/2015/12/04/christie-calls-out-cruz-paul-surveillance/76775374.

27 Press Release, Senator Bernie Sanders, Sanders Votes Against Patriot Act Extension (May 26, 2011), http://www.sanders.senate.gov/newsroom/press-releases/sanders-votes-against-patriot-act-extension ("I voted against extending the Patriot Act today for the same reason I voted against enacting it in 2001: it gives the government far too much power to spy on innocent United States citizens and provides for very little oversight or disclosure."). For the votes cast on the 2001 Patriot Act, *see* On Passage of the Bill, H.R. 3162 (Oct. 25, 2001), http://www.senate.gov/legislative/LIS/roll_call_lists/roll_call_vote_cfm.cfm?congress=107&session=1&vote=00313; Final Vote Results for Roll Call, H.R. 3162 (Oct. 21, 2001), http://clerk.house.gov/evs/2001/roll398.xml.

28 *Qaeda Front Group Claims Wave of Iraq Attacks,* The Times of Oman (Jan. 21, 2013), http://www.timesofoman.com/article/7313/World/Qaeda-front-group-claims-wave-of-Iraq-attacks.

29 Bassem Mroue & Maamoun Youssef, *Iraqi al-Qaeda and Syria Militants Announce Merger,* USA Today (Apr. 9, 2013), http://www.usatoday.com/story/news/world/2013/04/09/qaeda-iraq-syria-merger/2066333.

30 *Iraq: Hundreds Escape from Abu Ghraib Jail,* The Guardian (July 22, 2013), http://www.theguardian.com/world/2013/jul/22/iraq-prison-attacks-kill-dozens; Adam Schreck, *Abu Ghraib Prison Break: Al Qaeda In Iraq Claims Responsibility For Raid,* The World Post (July 23, 2013), http://www.huffingtonpost.com/2013/07/23/abu-ghraib-prison-break-al-qaeda-iraq_n_3639101.html.

31 Erika Solomon, *Islamist Rebels Capture Syria's Largest Oilfield: Activists,* Reuters (Nov. 23, 2013), http://www.reuters.com/article/2013/11/23/us-syria-crisis-oil-idUSBRE9AM03K20131123.

32 Liz Sly, *Al-Qaeda Force Captures Fallujah Amid Rise in Violence in Iraq,* Wash. Post (Jan. 3, 2014), https://www.washingtonpost.com/world/al-qaeda-force-captures-fallujah-amid-rise-in-violence-in-iraq/2014/01/03/8abaeb2a-74aa-11e3-8def-a33011492df2_story.html.

33 Ingrid Melander & Adrian Croft, *France Arrests Suspect in Brussels Jewish Museum Shooting,* Reuters (June 1, 2014), http://www.reuters.com/article/2014/06/01/us-belgium-shooting-france-idUSKBN0EC17P20140601.

34 *Iraqi City of Mosul Falls to Jihadists,* CBS News (June 10, 2014), http://www.cbsnews.com/news/iraq-city-of-mosul-falls-into-hands-of-isis-jihadists-after-police-army-abandon-posts; Paul D. Shinkman, *ISIL Declares Victory by Establishing Caliphate,* US News and World Report (June 30, 2014), http://www.usnews.com/news/articles/2014/06/30/isil-declares-victory-in-iraq-by-establishing-new-islamic-caliphate.

35 Matt Olsen, Dir., Nat'l Counterterrorism Ctr., Remarks (Sept. 3, 2014), http://www.odni.gov/files/documents/2014-09-03%20Remarks%20for%20the%20Brookings%20Institution.pdf.

36 Greg Bothelo, *ISIS Executes British Aid Worker David Haines; Cameron Vows Justice,* CNN (Sept. 14, 2014), http://www.cnn.com/2014/09/13/world/meast/isis-haines-family-message/index.html.

37 David Remnick, *Going the Distance,* The New Yorker (Jan. 27, 2014), http://www.newyorker.com/magazine/2014/01/27/going-the-distance-david-remnick. The *New Yorker* article was the one in which the president referred to ISIL as a "jayvee" group:

> The analogy we use around here sometimes, and I think is accurate, is if a jayvee team puts on Lakers uniforms that doesn't make them Kobe Bryant," Obama said, resorting to an uncharacteristically flip analogy. "I think there is a distinction between the capacity and reach of a bin Laden and a network that is actively planning major terrorist plots against the homeland versus jihadists who are engaged in various local power struggles and disputes, often sectarian.

In his May 2013 speech, the president gave a more nuanced assessment, without mentioning ISIL by name:

> Unrest in the Arab world has also allowed extremists to gain a foothold in countries like Libya and Syria. But here, too, there are differences from 9/11. In some cases, we continue to confront state-sponsored networks like Hezbollah that engage in acts of terror to achieve political goals. Other of these groups are simply collections of local militias or extremists interested in seizing territory. And while we are vigilant for signs that these groups may pose a transnational threat, most are focused on operating in the countries and regions where they are based. And that means we'll face more localized threats like what we saw in Benghazi, or the BP oil facility in Algeria, in which local operatives—perhaps in loose affiliation with regional networks—launch periodic attacks against Western diplomats, companies, and other soft targets, or resort to kidnapping and other criminal enterprises to fund their operations.

Remarks by the president at the National Defense University, *supra* note 6.

38 Meet the Press Transcript (Sept. 7, 2014), http://www.nbcnews.com/meet-the-press/meet-press-transcript-september-7-2014-n197866 ("ISIL poses a broader threat because of its territorial ambitions in Iraq and Syria").

39 Arlette Saenz, *President Obama Vows to 'Completely Decapitate' ISIS Operations,* ABC News (Nov. 13, 2013), http://abcnews.go.com/Politics/president-obama-vows-completely-decapitate-isis-operations/story?id=35173579 ("From the start our goal has been first to contain, and we have contained them.").

40 *See* John McLaughlin, *The Paris Attacks: Former CIA Chief Weighs In,* Ozy (Nov. 15, 2015), http://www.ozy.com/pov/the-paris-attacks-former-cia-chief-weighs-in/66155.

41 Saeed Al-Batati & Kareem Fahim, *War in Yemen is Allowing Qaeda Group to Expand,* N.Y. Times (Apr. 16, 2015), http://www.nytimes.com/2015/04/17/world/middleeast/khaled-bahah-houthi-rebel-yemen-fighting.html?_r=0; *Yemen Profile—Timeline,* BBC News (Nov. 25, 2015), http://www.bbc.com/news/world-middle-east-14704951; *How Instability in Yemen Affects the U.S.,* CBS News (Mar. 25, 2015), http://www.cbsnews.com/news/how-instability-in-yemen-affects-the-us; Yara Bayoumy, *Al Qaeda Thrives in Yemen amid Weak Security, Stalled Dialogue,* Reuters (Dec. 8, 2013), http://www.reuters.com/article/us-yemen-security-idUSBRE9B702520131208.

42 Maggie Michael, *Al-Qaida in the Arabian Peninsula Claims Responsibility for Paris Attack,* US News and World Report (Jan 14. 2015), http://www.usnews.com/news/world/articles/2015/01/14/yemens-al-qaida-claims-responsibility-for-paris-attack.

43 *Libya Profile—Timeline,* BBC News (Jan. 21, 2016), http://www.bbc.com/news/world-africa-13755445; Christopher Stephen, *ISIL's Rise in Libya,* Politico (Jan. 29, 2015), http://www.politico.com/magazine/story/2015/01/isils-rise-in-libya-114742; Ruth Sherlock & Colin Freeman, *Islamic State "Planning to use Libya as Gateway to Europe",* The Telegraph (Feb. 17, 2015), http://www.telegraph.co.uk/news/worldnews/islamic-state/11418966/Islamic-State-planning-to-use-Libya-as-gateway-to-Europe.html.

44 *See, e.g.*, Nils Muiznieks, Opinion, *Europe Is Spying on You,* N.Y. Times (Oct. 27, 2015), http://www.nytimes.com/2015/10/28/opinion/europe-is-spying-on-you-mass-surveillance.html; Mark Scott, *British Court Rules in Favor of Electronic Surveillance,* N.Y. Times (Dec. 5, 2014), http://www.nytimes.com/2014/12/06/world/europe/british-court-says-governments-electronic-surveillance-is-legal.html; Justin Ling, *New Mass Surveillance Laws Come to Canada, France, and the United Kingdom, as the NSA May Have its Wings Clipped,* Vice News (May 12, 2015), https://news.vice.com/article/new-mass-surveillance-laws-come-to-canada-france-and-the-united-kingdom-as-the-nsa-may-have-its-wings-clipped; Data Retention and Investigatory Powers Act 2014 (Gr. Brit.), http://www.legislation.gov.uk/ukpga/2014/27/contents/enacted.

45 Muiznieks, *supra* note 44. *See* Tonda MacCharles, *New Spy Bill Would let Canadian Agents Operate Illegally Abroad,* The Star (Oct. 27, 2014), http://www.thestar.com/news/canada/2014/10/27/new_spy_bill_would_let_canadian_agents_operate_illegally_abroad.html; Data Retention and Investigatory Powers Act 2014 (Gr. Brit.), http://www.legislation.gov.uk/ukpga/2014/27/contents/enacted.

46 The Draft Investigatory Powers Bill (Nov. 4, 2015) is available at https://www.gov.uk/government/publications/draft-investigatory-powers-bill.

47 *See, e.g.*, Jack Goldsmith, *The Forever War is Entrenched,* Lawfare (Oct. 19, 2015), https://www.lawfareblog.com/forever-war-entrenched; Jack Goldsmith, *President Obama's National Security Legacy After Paris,* Lawfare (Nov. 16, 2015), https://www.lawfareblog.com/president-obamas-national-security-legacy-after-paris.

48 For a more complete and very thoughtful assessment of the challenges posed by ISIL, *see Hearing: Outside Views on the Strategy for Iraq and Syria Before the H. Comm. on Armed Servs.,* 114th Cong. (2015) (statement of John McLaughlin), http://docs.house.gov/meetings/AS/AS00/20151118/104191/HHRG-114-AS00-Wstate-McLaughlinJ-20151118.pdf. In December 2015, a senior Treasury Department official is reported to have said that ISIL had taken between $500 million and $1 billion from banks in Syria and Iraq, and had earned more than $500 million from black-market oil sales. Jonathan Saul & Guy Faulconbridge, *U.S. Says Islamic State has Made $1.5 Billion from Bank Looting, Oil Sales,* Reuters (Dec. 10, 2015), http://www.reuters.com/article/us-mideast-crisis-syria-usa-idUSKBN0TT2IF20151210 (quoting Adam Szubin, acting undersecretary for terrorism and financial intelligence, US Department of the Treasury). For a discussion of ISIL affiliates in places such as Libya, Nigeria, the Sinai Peninsula, Saudi Arabia, Afghanistan, Pakistan, and Yemen, *see, e.g.*, Eric Schmitt & David D. Kirkpatrick, *Islamic State Sprouting Limbs Beyond Its Base,* N.Y. Times (Feb. 14, 2015), http://www.nytimes.com/2015/02/15/world/middleeast/islamic-state-sprouting-limbs-beyond-mideast.html; *Islamic State Moves in on Al-Qaeda Turf,* BBC News (June 26, 2015), http://www.bbc.com/news/world-31064300. For a discussion of ISIL's current chief of external operations, Abu Muhammed al-Adnani, *see, e.g.*, Robert Windrem, *America's Most Wanted: The ISIS Leader at the Top of the U.S. Kill List,* NBC News (Dec. 11, 2015), http://www.nbcnews.com/storyline/isis-uncovered/americas-most-wanted-isis-leader-top-u-s-kill-list-n477946.

49 *See, e.g.*, Luay Al-Khatteeb, *The UN Strikes Back at ISIL's Black Economy*, Brookings Inst. (Aug. 23, 2014), http://www.brookings.edu/research/opinions/2014/08/23-un-strikes-back-at-isil-black-economy.

50 Liz Sly, *How the Battle Against the Islamic State is Redrawing the Map of the Middle East,* Wash. Post (Dec. 30, 2015), https://www.washingtonpost.com/world/on-the-front-lines-of-the-war-against-the-islamic-state-a-tangled-web/2015/12/30/d944925a-9244-11e5-befa-99ceebcbb272_story.html.

51 *See* McLaughlin, *supra* note 40.

52 *See, e.g.*, Nathan Myhrvold, *Strategic Terrorism: A Call to Action,* https://lawfare.s3-us-west-2.amazonaws.com/staging/s3fs-public/uploads/2013/07/Strategic-Terrorism-Myhrvold-7-3-2013.pdf. ISIL has apparently used chemical weapons in Syria: *see* Raja Abdulrahim, *Islamic State Accused of New Chemical Weapons Attack in Syria,* Wall Street Journal (Aug. 23, 2015), http://www.wsj.com/articles/islamic-state

-accused-of-using-chemical-weapons-in-syria-1440353562. I am not aware of any credible, public reporting that ISIL has so far developed a meaningful capability in either biological or nuclear weapons.

53 *PCLOB 702 Report, supra* note 1, at 2.

54 *Id.* at 9.

55 *See* Privacy and Civil Liberties Oversight Bd, *Recommendations Assessment Report* 1 (2015) [hereinafter PCLOB 1-29-15 RAR], https://www.pclob.gov/library/Recommendations_Assessment-Report.pdf ("The Administration has accepted virtually all of the recommendations in the Board's Section 702 report and has begun implementing many of them.").

56 NSIP, *supra* note 2, § 17:5, (Supp. 2015). Section 702 of the FAA is codified at 50 U.S.C. § 1881a.

57 *See PCLOB 702 Report, supra* note 1, at 33–34, 84.

58 *See id.* at 37.

59 *Id.* at 10; *see id.* at 38 ("There are technical reasons why 'about' collection is necessary to acquire even some communications that are 'to' and 'from' a tasked selector. In addition, some types of 'about' communications actually involve Internet activity of the targeted person. The NSA cannot, however, distinguish in an automated fashion between 'about' communications that involve the activity of the target from communications that, for instance, merely contain an email address in the body of an email between two non-targets." (footnotes omitted)).

60 For a detailed discussion of the two FISA Court decisions from 2011, *see* NSIP, *supra* note 2, § 17:5 (Supp. 2015).

61 *Id.* (quoting [REDACTED], 2011 WL 10945618, at *13 (FISA Ct. Oct. 3, 2011)).

62 *See id.* (citing *PCLOB 702 Report, supra* note 1, at 84–86).

63 *See PCLOB 702 Report, supra* note 1, at 143–145 ("To build on current efforts to filter upstream communications to avoid collection of purely domestic communications, the NSA and DOJ, in consultation with affected telecommunications service providers, and as appropriate, with independent experts, should periodically assess whether filtering techniques applied in upstream collection utilize the best technology consistent with program needs to ensure government acquisition of only communications that are authorized for collection and prevent the inadvertent collection of domestic communications. . . . The NSA periodically should review the types of communications acquired through 'about' collection under Section 702, and study the extent to which it would be technically feasible to limit, as appropriate, the types of 'about' collection."); PCLOB 1-29-15 RAR, *supra* note 55, at 21–24.

64 NSIP, *supra* note 2, § 17:5 (Supp. 2015). As the PCLOB explained in its report on FAA § 702,

> In a still-classified September 2008 opinion, the FISC agreed with the government's conclusion that the government's target when it acquires an "about" communication is not the sender or recipients of the communication, regarding whom the government may know nothing, but instead the targeted user of the Section 702–tasked selector. The FISC's reasoning relied upon language in a congressional report, later quoted by the FISA Court of Review, that the "target" of a traditional FISA electronic surveillance "is the individual or entity . . . about whom or from whom information is sought."

PCLOB 702 Report, supra note 1, at 29–30. It is certainly true that the "target" of surveillance is the person from or about whom the government is seeking information, as discussed in NSIP, *supra* note 2, §§ 7:13, 8:1, 17:5. But that does not resolve the question whether the government can review the contents of an unlimited number of e-mails from unrelated parties in its effort to find information "about" the target.

65 The Obama administration certainly has described itself as restricting surveillance in favor of privacy. *See, e.g.*, ODNI Signals Intelligence Reform 2015 Anniversary Report, http://icontherecord.tumblr.com/ppd-28/2015/privacy-civil-liberties. For a more complete discussion of PPD-28, *see* NSIP, *supra* note 2, § 19:4.50 (Supp. 2015).

66 Under current law, queries of FAA § 702 data are governed by minimization procedures approved by the FISA Court. As explained in the PCLOB's report on Section 702:

> Each agency that receives communications under Section 702 has its own minimization procedures, approved by the FISA court, that govern the agency's use, retention, and dissemination of Section 702 data. Among other things, these procedures include rules on how the agencies may "query" the collected data. The NSA, CIA, and FBI minimization procedures all include provisions permitting these agencies to query data acquired through Section 702, using terms intended to discover or retrieve communications content or metadata that meets the criteria specified in the query. These queries may include terms that identify specific U.S. persons and can be used to retrieve the already acquired communications of specific U.S. persons. Minimization procedures set forth the standards for conducting queries. For example, the NSA's minimization procedures require that queries of Section 702–acquired information be designed so that they are "reasonably likely to return foreign intelligence information."

PCLOB 702 Report, supra note 1, at 7–8 (footnotes omitted). For a discussion of the mechanics of querying, *see id.* at 55–60.

67 *See* Charlie Savage, New York Times, statement at The Second Annual Cato Surveillance Conference, After FREEDOM: A Dialogue on NSA in the Post-Snowden Era (Oct. 21. 2015) ("the FISA Amendments Act come [sic] up for renewal in 2017, and . . . there is an effort already in Congress to require warrants before the government can look at already-collected information that it gathered without a warrant for an American's identifier, which is something the intelligence community has been resisting. But we'll see—that, I imagine, is the next battle").

68 *PCLOB 702 Report, supra* note 1, at 57. With thanks to an attentive journalist for the reference, during 2013, CIA conducted "fewer than 1900" queries of the data for U.S. person information (some of them on behalf of other U.S. agencies), of which "[a]pproximately 27 percent . . . were duplicative or recurring queries conducted at different times using the same identifiers," and FBI conducted a "substantial" but unspecified number of queries during 2013. *See* Letter from Deirdre M. Walsh, Director, Office of Legislative Affairs, Office of the Director of National Intelligence, to Senator Ron Wyden (June 27, 2014), available at https://www.documentcloud.org/documents/2095183-odni-letter-to-wyden-2014.html.

69 *See* Minimization Procedures used by the National Security Agency in Connection with Acquisitions of Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, as Amended, § 3(b)(5) (Oct. 31, 2011), http://www.dni.gov/files/documents/Minimization%20Procedures%20used%20by%20NSA%20in%20Connection%20with%20FISA%20SECT%20702.pdf; *PCLOB 702 Report, supra* note 1, at 7 ("Data from upstream collection is received only by the NSA: neither the CIA nor the FBI has access to unminimized upstream data."); *PCLOB 702 Report, supra* note 1, at 35, 161 n.571.

70 *PCLOB 702 Report, supra* note 1, at 12; *see also id.* at 137–138.

71 In February 2015, ODNI reported that

> FBI, CIA, and NSA each are instituting new requirements for using a U.S. person identifier to query information acquired under Section 702. As recommended by the Privacy and Civil Liberties Oversight Board, NSA's minimization procedures will require a written statement of facts showing that a query is reasonably likely to return foreign intelligence information. CIA's minimization procedures will be similarly amended to require a statement of facts for queries of content. In

> addition, FBI's minimization procedures will be updated to more clearly reflect the FBI's standard for conducting U.S. person queries and to require additional supervisory approval to access query results in certain circumstances.

ODNI Signals Intelligence Reform 2015 Anniversary Report, http://icontherecord.tumblr.com/ppd-28/2015/privacy-civil-liberties; *see also* PCLOB 1-29-15 RAR at 19–20. Other possibilities are set out in NSIP:

> As to querying of downstream data, there are several options available in devising the new restrictions. Substantively, the government could simply forbid querying altogether, or forbid it when motivated by an affirmative (rather than protective) foreign intelligence purpose. Alternatively, or in addition, it could adopt a procedural approach, requiring a finding of reasonable articulable suspicion (RAS), or even probable cause, that the U.S. person is associated in some way with an international terrorist group, or perhaps another foreign power. Such a finding could be made either by the Executive Branch unilaterally, or be subject to approval by the FISA Court (perhaps with an emergency exception), before querying may occur.

NSIP, *supra* note 2, § 19:4.50 (Supp. 2015).

72 *PCLOB 702 Report, supra* note 1, at 14. For more detail on how querying works under Section 702, *see id.* at 55–60.

73 50 U.S.C. § 1861(b)(2)(C).

74 *See PCLOB 702 Report, supra* note 1, at 137–138.

75 *ODNI Signals Intelligence Reform 2015 Anniversary Report,* http://icontherecord.tumblr.com/ppd-28/2015/privacy-civil-liberties. In particular, according to Robert Litt, the General Counsel of ODNI:

> Under the new policy, in addition to any other limitations imposed by applicable law, including FISA, any communication to or from, or information about, a U.S. person acquired under Section 702 of FISA shall not be introduced as evidence against that U.S. person in any criminal proceeding except (1) with the prior approval of the Attorney General and (2) in (A) criminal proceedings related to national security (such as terrorism, proliferation, espionage, or cybersecurity) or (B) other prosecutions of crimes involving (i) death; (ii) kidnapping; (iii) substantial bodily harm; (iv) conduct that constitutes a criminal offense that is a specified offense against a minor as defined in 42 USC 16911; (v) incapacitation or destruction of critical infrastructure as defined in 42 USC 5195c(e); (vi) cybersecurity; (vii) transnational crimes; or (vii) human trafficking.

Robert S. Litt, Gen. Counsel, ODNI, Prepared Remarks on Signals Intelligence Reform at the Brookings Institute (Feb. 4, 2015), http://icontherecord.tumblr.com/post/110632851413/odni-general-counsel-robert-litts-as-prepared.

76 *PCLOB 702 Report, supra* note 1, at 97 n.438.

77 *Id.* at 162.

78 *See* Anthony Faiola & Souad Mekhennet, *The Islamic State Creates a New Type of Jihadist: Part Terrorist, Part Gangster,* Wash. Post (Dec. 20, 2015), https://www.washingtonpost.com/world/europe/the-islamic-state-creates-a-new-type-of-jihadist-part-terrorist-part-gangster/2015/12/20/1a3d65da-9bae-11e5-aca6-1ae3be6f06d2_story.html; Andrew Higgins & Kimiko de Freytas-Tamura, *An ISIS Militant From Belgium Whose Own Family Wanted Him Dead,* N.Y. Times (Nov. 17, 2015), http://www.nytimes.com/2015/11/18/world/europe/paris-attacks-abdelhamid-abaaoud-an-isis-militant-from-belgium-whose-own-family-wanted-him-dead.html (describing alleged petty crime, and drug dealing, by some of the Paris attackers); *cf.* Lorenzo Vidino & Seamus Hughes, Program on Extremism, George Wash. Univ., *ISIS in America: From Retweets to Raqqa* (2015), http://cchs.gwu.edu/isis-in-america.

79 *See* NSIP, *supra* note 2, § 19:4.50 (Supp. 2015) and sources cited therein. Even if some querying of data collected under EO 12333 were subject to a probable-cause or other requirement, it is not clear that the same requirement would apply to data collected under FAA § 702 because of the higher standards and requirements for collection under Section 702.

80 *Cf.* United States v. Ramirez, 523 U.S. 65, 71 (1998) ("This is not to say that the Fourth Amendment speaks not at all to the manner of executing a search warrant. The general touchstone of reasonableness which governs Fourth Amendment analysis, governs the method of execution of the warrant. Excessive or unnecessary destruction of property in the course of a search may violate the Fourth Amendment, even though the entry itself is lawful and the fruits of the search are not subject to suppression." (citation omitted)). In its decision upholding "upstream" collection, discussed above, the FISA Court relied in part on strong minimization procedures to uphold very broad acquisition of information. *See* NSIP, *supra* note 2, § 17:5 (Supp. 2015); *see also* United States v. Mohamud, No. 10-475, 2014 WL 2866749, at *26 (D. Or. June 24, 2014) ("Thus, subsequent querying of a § 702 collection, even if U.S. person identifiers are used, is not a separate search and does not make § 702 surveillance unreasonable under the Fourth Amendment."). The analysis under the FAA may not be the same as earlier analysis governing EO 12333 surveillance, in part because of the role of the FISA Court in the former.

81 *See* Minimization Procedures used by the National Security Agency in Connection with Acquisitions of Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, as Amended, § 8 (Oct. 31, 2011), http://www.dni.gov/files/documents/Minimization%20Procedures%20used%20by%20NSA%20in%20Connection%20with%20FISA%20SECT%20702.pdf; *see also* NSIP, *supra* note 2, § 9:8.50 (Supp. 2015). For a discussion of minimization in general, *see* NSIP, *supra* note 2, ch. 9.

82 *See* Case C-362/14, Schrems v. Data Prot. Comm'r, ¶¶ 11, 94–98 (Oct. 6, 2015), http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117en.pdf.

83 *Cf., e.g.,* David Anderson, *A Question of Trust: Report of the Investigatory Powers Review* (2015), https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2015/06/IPR-Report-Print-Version.pdf (discussing UK and European surveillance standards).

84 *PCLOB 702 Report, supra* note 1, at 52.

85 *See id.* at 55–56 ("The NSA . . . often stores data acquired from multiple legal authorities in a single data repository. Instead of limiting access to whole databases, the NSA tags each acquired communication with the legal authority under which it was acquired, and then has systems that prevent an analyst from accessing or querying data acquired under a legal authority for which the analyst does not have the requisite training").

86 *What We Do,* Off. Director of Nat'l Intelligence, http://www.dni.gov/index.php/about/organization/chief-information-officer-what-we-do. The ODNI CIO reports:

> The IC ITE [Intelligence Community Integrated Intelligence Enterprise] represents a strategic shift from agency-centric information technology (IT) to a common enterprise platform where the IC can easily and securely share technology, information, and capabilities across the Community. To enable this change, the Director of National Intelligence (DNI), in consultation with the applicable IC element head, has designated IC elements as Service Providers, who assume the responsibility for developing and maintaining IC ITE services of common concern. IC ITE Services are the capabilities and shared solutions that are being delivered across the IC to help complete the vision of IC ITE. These services currently include: a common desktop environment; a joint cloud environment; an applications mail; an enterprise management capability; identification, authentication, and authorization capabilities; network requirements and engineering services; and a security coordination service.

> Working with the IC under the IC ITE Strategy, the IC CIO is facilitating the development, implementation, and adoption of seamless and secure enterprise solutions that promote trusted collaboration—connecting people to people, people to data, and data to data. The strategy enhances the IC's ability to securely discover, access, and share information across agencies and ultimately enables greater mission success.
>
> IC ITE Implementation is an evolving process of consolidating and adopting Community capabilities. With the adoption of IC ITE Services, users will have broader and faster access to data and an increased ability to collaborate on common systems across the IC in ways that enhance mission integration and optimize mission success.

Id.

87 *See* 50 U.S.C. §§ 1801(e)(1)–(2), 1881a(a), 1881a(g)(2)(A)(v).

88 For a discussion of "foreign intelligence information" including both "protective" and "affirmative" intelligence, *see* NSIP, *supra* note 2, §§ 8:29–8:36. For a discussion of PPD-28, *see* NSIP, *supra* note 2, § 19:4.50 (Supp. 2015).

89 *See* Press Release, Privacy and Civil Liberties Oversight Bd., *PCLOB Announces Its Short-Term Agenda* (Sept. 3, 2014), http://www.pclob.gov/newsroom/20140807.html ("The Board will examine EO 12333 and its implications for privacy and civil liberties."); *see also* PCLOB Examination of E.O. 12333 Activities in 2015, https://www.pclob.gov/library/20150408-EO12333_Project_Description.pdf (discussing plans for public report on E.O. 12333). Executive Order 12333, 3 C.F.R. 200 (1982), was issued on December 4, 1981. It was amended on August 27, 2004 by Executive Order 13355, 3 C.F.R. 218 (2004). It was again amended on July 30, 2008 by Executive Order 13470, 3 C.F.R. 218 (2009). For a discussion of EO 12333 and its impact on the U.S. Intelligence Community, including intelligence surveillance, *see* NSIP, *supra* note 2, chs. 1, 2, 17.

90 For a discussion of this possibility, and how it influenced the adoption of the first executive order comprehensively regulating the Intelligence Community, an antecedent to EO 12333, *see id.* §§ 1:4, 2:7. More recently, in December 2014, in Section 309 of the Intelligence Authorization Act for Fiscal Year 2015, Pub. L. No. 113-293, 128 Stat. 3998 (codified at 50 U.S.C. § 1813 (Supp. II 2014)), Congress required by statute procedures governing retention of communications acquired under EO 12333. To my knowledge, this is the first direct statutory regulation of such surveillance.

91 *See* David Perera, *Terror Fears Don't Budge Obama on Encryption,* Politico (Dec. 17, 2015), http://www.politico.com/story/2015/12/obama-resists-calls-for-encryption-shift-216920; Ellen Nakashima, *After Terrorist Attacks, the Debate Over Encryption Gets New Life,* Wash. Post (Dec. 9, 2015), https://www.washingtonpost.com/world/national-security/after-terrorist-attacks-the-debate-over-encryption-gets-new-life/2015/12/09/3bb73f22-9e99-11e5-8728-1af6af208198_story.html; Ellen Nakashima & Andrea Peterson, *Obama Administration Opts Not to Force Firms to Decrypt Data—For Now,* Wash. Post (Oct. 8, 2015), https://www.washingtonpost.com/world/national-security/obama-administration-opts-not-to-force-firms-to-decrypt-data--for-now/2015/10/08/1d6a6012-6dca-11e5-aa5b-f78a98956699_story.html.

92 Much of the most sophisticated and thoughtful material on encryption is available on or through Lawfare, www.lawfareblog.com.

93 50 U.S.C. § 1805(c)(2)(B); *see also id.* §§ 1802(a)(4)(A), 1822(a)(4)(A)(i), 1842(d)(2)(B)(i); 50 U.S.C.A. 1861(c)(2)(F)(vi). The language in FISA is very similar to that in a 1970 amendment to the Wiretap Act, which provides that an

> order authorizing the interception of a wire, oral, or electronic communication under this chapter shall, upon request of the applicant, direct that a provider of wire or electronic communication service, landlord, custodian or other person shall furnish the applicant forthwith all information,

> facilities, and technical assistance necessary to accomplish the interception unobtrusively and with a minimum of interference with the services that such service provider, landlord, custodian, or person is according the person whose communications are to be intercepted.

18 U.S.C. § 2518(4); *see also id.* § 2511(2)(a)(ii).

94 The term is defined in 50 U.S.C. § 1881(b)(4) to include:

> (A) a telecommunications carrier, as that term is defined in [section 3 of the Communications Act of 1934 (47 U.S.C. 153)];
>
> (B) a provider of electronic communication service, as that term is defined in section 2510 of title 18, [United States Code];
>
> (C) a provider of a remote computing service, as that term is defined in section 2711 of title 18, [United States Code];
>
> (D) any other communication service provider who has access to wire or electronic communications either as such communications are transmitted or as such communications are stored; or
>
> (E) an officer, employee, or agent of an entity described in subparagraph (A), (B), (C), or (D).

50 U.S.C. § 1881(b)(4).

95 *Id.* § 1881a(h)(1)(A).

96 *See id.* § 1881a(g)(2)(A)(vi).

97 *See id.* § 1881b(a)(1). A Section 703 order "shall direct . . . if applicable, an electronic communication service provider to provide to the Government forthwith all information, facilities, or assistance necessary to accomplish the acquisition authorized under such order in a manner that will protect the secrecy of the acquisition and produce a minimum of interference with the services that such electronic communication service provider is providing to the target of the acquisition." *Id.* § 1881b(c)(5)(B).

98 *See id.* § 1881c(c)(3)(A).

99 434 U.S. 159 (1977).

100 28 U.S.C. § 1651.

101 *New York Tel. Co.,* 434 U.S. at 176–177. The Supreme Court elaborated on this point in a footnote:

> We reject the Court of Appeals' suggestion that the fact that Congress amended Title III [the Wiretap Act] to require that communication common carriers provide necessary assistance in connection with electronic surveillance within the scope of Title III reveals a congressional "doubt that the courts possessed inherent power to issue such orders" and therefore "it seems reasonable to conclude that similar authorization should be required in connection with pen register orders. . . ." The amendment was passed following the decision of the Ninth Circuit in *Application of United States,* 427 F.2d 639 (1970), which held that absent specific statutory authority, a United States District Court was without power to compel a telephone company to assist in a wiretap conducted pursuant to Title III. The court refused to infer such authority in light of Congress' silence in a statute which constituted a "comprehensive legislative treatment" of wiretapping. We think that Congress' prompt action in amending the Act was not an acceptance of the Ninth Circuit's view but "more in the nature of an overruling of that opinion." The meager legislative history of the amendment indicates that Congress was only providing an unequivocal statement of its intent under Title III. *See* 115 Cong. Rec. 37192 (1969) (remarks of Sen. McClellan). We decline to infer from a congressional grant of authority under these circumstances that such authority was previously lacking.

> Moreover, even if Congress' action were viewed as indicating acceptance of the Ninth Circuit's view that there was no authority for the issuance of orders compelling telephone companies to provide assistance in connection with wiretaps without an explicit statutory provision, it would not follow that explicit congressional authorization was also needed to order telephone companies to assist in the installation and operation of pen registers which, unlike wiretaps, are not regulated by a comprehensive statutory scheme. In any event, by amending Title III Congress has now required that at the Government's request telephone companies be directed to provide assistance in connection with wire interceptions. It is plainly unlikely that Congress intended at the same time to leave federal courts without authority to require assistance in connection with pen registers.

Id. at 177 n.25 (some citations omitted).

102 This is in one sense the continuation of a trend revealed publicly by the US government before the FAA. *See* NSIP, *supra* note 2, § 16:5 (quoting remarks by Ken Wainstein).

103 The Communications Assistance for Law Enforcement Act, 47 U.S.C. §§ 1001–1010. Under one provision of CALEA, a "telecommunications carrier shall not be responsible for decrypting, or ensuring the government's ability to decrypt, any communication encrypted by a subscriber or customer, unless the encryption was provided by the carrier and the carrier possesses the information necessary to decrypt the communication." *Id.* § 1002(b)(3),

104 *See* Quinta Jurecic, *DOJ and Apple File Briefs in EDNY Encryption Case,* Lawfare (Oct. 26, 2015), https://www.lawfareblog.com/doj-and-apple-file-briefs-edny-encryption-case; *see also* H.R. Rep. No. 103-827, pt. 1, at 15 (1994) ("While the Supreme Court has read [18 U.S.C. § 2518(4)] as requiring the Federal courts to compel, upon request of the government, 'any assistance necessary to accomplish an electronic interception,' *United States v. New York Telephone,* 434 U.S. 159, 177 (1977), the question of whether companies have any obligation to design their systems such that they do not impede law enforcement interception has never been adjudicated").

105 *In re* U.S. for an Order Authorizing Roving Interception of Oral Communications, 349 F.3d 1132, 1145 (9th Cir. 2003).

106 *Id.* at 1147–48 (Tallman, J., dissenting) (citations omitted).

107 *See Current Membership—Foreign Intelligence Surveillance Court of Review,* U.S. Foreign Intelligence Surveillance Court, http://www.fisc.uscourts.gov/fiscr_membership.

108 Apple Inc.'s Response to Court's October 9, 2015 Memorandum and Order at 4, *In re* Order Requiring Apple Inc. to Assist in the Execution of a Search Warrant Issued by this Court, No. 15 MISC 1902 (JO) (E.D.N.Y. Oct. 19, 2015), https://www.lawfareblog.com/doj-and-apple-file-briefs-edny-encryption-case.

109 Draft Investigatory Powers Bill at 16 (Nov. 2015) (U.K.) (hereinafter UK Draft IP Bill), https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/473770/Draft_Investigatory_Powers_Bill.pdf. This is distinct from equipment interference whose primary purpose is not collection of information, but rather something like destruction of data. *See id.* at 236 (explanatory notes).

110 Written Evidence (IPB0119), Electronic Frontier Foundation, Comment 3 (Dec. 21, 2015) [hereinafter EFF UK Comments], http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/draft-investigatory-powers-bill-committee/draft-investigatory-powers-bill/written/26370.html.

111 *Id.*, Comment 27.

112 *Id.*, Comment 24. This possibility raises an interesting question that Congress may want to consider with respect to the technical assistance provisions of the FAA. As noted above, traditional FISA allows compelled assistance from "a specified communication or other common carrier, landlord, custodian, or

other specified person," while FAA § 702 applies only to an "electronic communication service provider" (ECSP). The question is whether an ECSP is subject to the compelled assistance provisions of FAA § 702 where it is not directly involved in facilitating the communications to be monitored—e.g., if Microsoft were compelled to push down a Windows software update to facilitate surveillance of a person who was sending encrypted emails on a Dell personal computer using a Comcast connection to the Internet and Gmail. For a discussion of a more extreme scenario, in which a Verizon employee is compelled to assist in a physical search under FAA § 702 by disabling a home alarm system, *see* NSIP, *supra* note 2, § 17:8.

113 EFF UK Comments, *supra* note 109, Comment 33.

114 *See* UK Draft IP Bill, *supra* note 109, at 237 (explanatory notes). A law passed by China in late December 2015 apparently requires technical assistance, including with decryption. *See* Benjamin Bissell, *What China's Anti-Terrorism Legislation Actually Says,* Lawfare (Dec. 30, 2015), https://www.lawfareblog.com/what-chinas-anti-terrorism-legislation-actually-says.

115 *See* Public Filings—U.S. Foreign Intelligence Surveillance Court, available at http://www.fisc.uscourts.gov/public-filings. According to Google, it provided at least some data in response to 76 percent of all worldwide government law enforcement requests for information in the six-month period ending December 31, 2010, as compared to 63 percent of such requests in the six-month period ending June 30, 2015, a reduction of 13 percent. Google assures users that it "review[s] each request to make sure that it complies with both the spirit and the letter of the law" and that it "may refuse to produce information or try to narrow the request in some cases." Google Transparency Report, https://www.google.com/transparencyreport/userdatarequests. Other companies report data on their compliance over a shorter period, making identification of trends more difficult. Apple's transparency report is available at http://images.apple.com/privacy/docs/government-information-requests-20150914.pdf, Facebook's transparency report is available at https://govtrequests.facebook.com, Yahoo!'s transparency report is available at https://transparency.yahoo.com/government-data-requests/index.htm, and Twitter's transparency report is available at https://transparency.twitter.com/information-requests/2015/jan-jun.

In describing their compliance qualitatively, however, these providers are often quite explicit in their efforts to provide as little data as possible to the government, and only when compelled to do so. Apple reports its approach to compliance as follows:

> Any government agency demanding customer content from Apple must get a search warrant. When we receive such a demand, our legal team carefully reviews it. If there's a question about the legitimacy or scope of the request we challenge it, as we have done as recently as this year. We only comply with information requests once we are satisfied that the request is valid and appropriate, and then we deliver the narrowest possible set of information.

Facebook describes itself as follows:

> We have strict processes in place to handle these government requests. Every request we receive is checked for legal sufficiency. We require officials to provide a detailed description of the legal and factual basis for their request, and we push back when we find legal deficiencies or overly broad or vague demands for information. We frequently share only basic subscriber information.

Yahoo! uses similar language to describe its approach:

> We carefully scrutinize each request to make sure that it complies with the law, and we push back on those requests that don't satisfy our rigorous standards. When we are compelled to disclose data, consistent with our Global Principles for Responding to Government Requests, we disclose only as much data as is necessary to comply with the request.

Yahoo! also highlights on its transparency web site a quote from its general counsel: "We fight any requests that we deem unclear, improper, overbroad, or unlawful."

Finally, Twitter reports this:

> We may not comply with requests for a variety of reasons. For example:
>
> We do not comply with requests that fail to identify a Tweet or Twitter account.
>
> We may seek to narrow requests that are overly broad.
>
> In other cases, users may have challenged the requests after we've notified them.

On the other hand, it is reasonably clear from these reports that the providers have not decided to resist government directives wholesale or to engage in broad civil disobedience of court orders. According to their latest published data, Google, Apple, Facebook, Yahoo! and Twitter all currently provide at least some information in response to approximately 80 percent of US government law enforcement requests. The companies do not appear to publish data on their compliance with US national security requests, although 50 U.S.C. § 1874 as amended by the USA Freedom Act has expanded reporting options.

116 *See* Microsoft's Objections to the Magistrate's Order Denying Microsoft's Motion to Vacate In Part a Search Warrant Seeking Customer Information Located Outside the United States at 5–6, *In re a Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corporation,* No. 13-MAG-2814; M9-150 (S.D.N.Y., June 6, 2014), http://www.washingtonpost.com/r/2010-2019/WashingtonPost/2014/06/10/National-Security/Graphics/SDNY%20MSFT%20Brief.pdf. Here is Microsoft's explanation for why it stores some users' e-mail in Ireland (citations omitted):

> In September 2010, Microsoft began to store data for certain web-based email accounts in a datacenter in Dublin, Ireland, which is leased and operated by Microsoft's wholly owned Irish subsidiary. The addition of the Dublin datacenter boosted the quality of service to numerous users because it reduces "network latency"—i.e., the inverse ratio between quality of service and the distance between a user and the datacenter where that user's account is hosted. Maximizing quality of service by minimizing network latency is critical to Microsoft's business. The Dublin datacenter allows Microsoft to reduce network latency and improve the quality of service for users located closer to Ireland than to the United States. For Outlook.com accounts stored in Dublin, the users' content resides on a specific server in the Dublin datacenter. It does not exist in any form inside the United States. Certain non-content information and address book data, in contrast, is stored in the United States.

For its part, the government says that "[a]ccording to Microsoft, it stores email content in a foreign datacenter when a subscriber claims to be physically present in an overseas location, but it takes no steps to confirm whether the subscriber is, in fact, logging in from a foreign location." Government's Memorandum of Law in Opposition to Microsoft's Motion to Vacate Email Account Warrant at 2, *In re a Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corporation,* No. 13-MAG-2814; M9-150 (S.D.N.Y., April 20, 2014), http://digitalconstitution.com/wp-content/uploads/2014/11/government-warrant.pdf

117 For a more complete discussion of these points, *see* NSIP, *supra* note 2, at §§ 7:12, 7:16, 7:18.

118 *See* NSIP, *supra* note 2, § 16:5 (quoting remarks by Ken Wainstein).

119 *See* NSIP, *supra* note 2, § 7:29. As a former assistant attorney general for national security (Ken Wainstein) explained in 2008 in a slightly different context, "We rely on the communications providers to do our intelligence surveillances. We can't do [the surveillances] without them because . . . we . . . don't own the communications systems. We need to rely on their assistance." Cited in NSIP, *supra* note 2, § 16:5. The full quotation from Wainstein reflects the fact that in some cases (but not in all), the government can obtain a FISA Court order.

120 *See* 18 U.S.C. § 2511(2)(a)(ii).

121 A good deal of high-quality scholarship, and also a short piece that I wrote on the subject, can be found on Lawfare, https://lawfareblog.com/search/node/cross-border%20data%20requests.

122 *See* Tor Project, https://www.torproject.org; Dune Lawrence, *The Inside Story of Tor, the Best Internet Anonymity Tool the Government Ever Built,* Bloomberg Business (Jan. 23, 2014), http://www.bloomberg.com/bw/articles/2014-01-23/tor-anonymity-software-vs-dot-the-national-security-agency.

123 For a discussion of the efforts of Netflix and Hulu to defeat VPN-spoofed IP addresses, *see, e.g.*, Thorin Klosowski, *Get Around Location Restrictions on Netflix or Hulu with a Private VPN IP Address,* Lifehacker (Jan. 20, 2016), http://lifehacker.com/get-around-location-restrictions-on-netflix-or-hulu-wit-1754043343.

124 *See* PCLOB 702 Report, *supra* note 1, at 38 ("NSA is required to use other technical means, such as Internet protocol ('IP') filters, to help ensure that at least one end of an acquired Internet transaction is located outside the United States."), 120 ("In part to compensate for this problem, the NSA takes additional measures with its upstream collection to ensure that no communications are acquired that are entirely between people located in the United States. These measures can include, for instance, employing Internet protocol filters to acquire only communications that appear to have at least one end outside the United States."); 132 n.544 (NSA masks U.S. person identities in its FAA § 702 reporting in certain circumstances, and unmasking can include IP addresses as well as names). *See also* NSA Director of Civil Liberties and Privacy Office Report, *NSA's Implementation of Foreign Intelligence Surveillance Act Section 702,* at 5–6 (April 16, 2014) ("For example, in certain circumstances NSA's procedures require that it employ an Internet Protocol filter to ensure that the target is located overseas"), http://www.dni.gov/files/documents/0421/702%20Unclassified%20Document.pdf.

125 Margaret Coker, Sam Schechner and Alexis Flynn, *How Islamic State Teaches Tech Savvy to Evade Detection,* Wall Street Journal (Nov. 16, 2015) ("Islamic State, for its part, has built a tech-savvy division of commanders who issue tutorials to sympathizers about the most secure and least expensive ways of communicating"), http://www.wsj.com/articles/islamic-state-teaches-tech-savvy-1447720824.

126 PCLOB 702 Report, *supra* note 1, at 117–118 (footnotes omitted).

127 PCLOB 702 Report, *supra* note 1, at 43–44 (emphasis and footnotes omitted).

128 NSA Director of Civil Liberties and Privacy Office Report, *NSA's Implementation of Foreign Intelligence Surveillance Act Section 702* at 4 (Apr. 16, 2014), http://www.dni.gov/files/documents/0421/702%20Unclassified%20Document.pdf.

129 According to one study from June 2015, VPNs are used by approximately 20 percent of European Internet users, but 11 out of 14 VPN providers studied leaked information about users because of the "IPv6 leakage." *See* Science Daily, *Most Internet Anonymity Software Leaks Users' Details* (June 29, 2015), http://www.sciencedaily.com/releases/2015/06/150629210621.htm.

130 *See* David Kris, *Thoughts on a Blue Sky Overhaul of Surveillance Laws,* Lawfare (May 2013), https://www.lawfareblog.com/thoughts-blue-sky-overhaul-surveillance-laws-introduction.

131 The Internet can be measured by number of users, amount of data, or number of web sites, among other things. Precise measurements can be difficult, but the trends are unmistakable. *See, e.g.*, Internet World Stats, *Internet Growth Statistics,* http://www.internetworldstats.com/emarketing.htm; Internet Live Stats, *Internet Users,* http://www.internetlivestats.com/internet-users.

132 Telegeography, *Global Bandwidth Research Service,* https://www.telegeography.com/research-services/global-bandwidth-research-service/index.html.

133 Robin Emmott, *Brazil, Europe Plan Undersea Cable to Skirt U.S. Spying,* Reuters (Feb. 24, 2014), http://www.reuters.com/article/2014/02/24/us-eu-brazil-idUSBREA1N0PL20140224.

134 *See* NSIP, *supra* note 2, § 16:12; Church Report Book III at 741.

135 Marc Ambinder, *How the U.S. Lost its Home Field Advantage,* The Atlantic (Feb. 6, 2010), http://www.theatlantic.com/politics/archive/2010/02/how-the-us-lost-its-home-field-surveillance-advantage/35495.

136 *See* David Kris, *What's the Big Secret,* Slate (Aug. 29, 2007), http://www.slate.com/articles/life/the_breakfast_table/features/2007/whats_the_big_secret/searching_the_haystacks.html.

137 *See* NSIP, *supra* note 1, Chapters 7, 16, 17.

138 For an overview of the Internet of Things, *see, e.g.*, *Internet of Things,* Wikipedia, https://en.wikipedia.org/wiki/Internet_of_Things.

139 For an overview of FinTech, *see Financial Technology,* Wikipedia, https://en.wikipedia.org/wiki/Financial_technology. For a thoughtful article on the future of FinTech, *see The Fintech Revolultion*, The Economist (May 9, 2015), http://www.economist.com/news/leaders/21650546-wave-startups-changing-financefor-better-fintech-revolution.

140 *See, e.g.*, Danny Yadron, *Iranian Hackers Infiltrated New York Dam in 2013,* Wall Street Journal (Dec, 20, 2015), http://www.wsj.com/articles/iranian-hackers-infiltrated-new-york-dam-in-2013-1450662559; Robert O'Harrow, Jr, *Cyber Search Engine Shodan Exposes Industrial Control Systems to New Risks,* Wash. Post (June 3, 2012), https://www.washingtonpost.com/investigations/cyber-search-engine-exposes-vulnerabilities/2012/06/03/gJQAIK9KCV_story.html.

141 *See, e.g.*, Susan Hennessey, *The Problems CISA Solves: ECPA Reform in Disguise,* Lawfare (Dec. 23, 2015), https://www.lawfareblog.com/problems-cisa-solves-ecpa-reform-disguise; Paul Rosenzweig, *The Cybsersecurity Act of 2015,* Lawfare (Dec. 16, 2015), https://www.lawfareblog.com/cybersecurity-act-2015.

142 *See, e.g.*, the reference to "common carrier" in 50 U.S.C. §§ 1801(*l*), 1802(a)(4), and 1805(c)(2)(B), and the definition and reference to "electronic communication service provider" in 50 U.S.C. § 1881(b)(4) and, *e.g.*, 50 U.S.C. § 1881a(g)(2)(A)(vi).

143 *See, e.g.*, Ben Bain, *Committee Sets Goals for Open-Source Info,* FCW (Sept. 11, 2008), https://fcw.com/articles/2008/09/11/committee-sets-goals-for-opensource-info.aspx.

144 In a November 2015 speech, for example, Hillary Clinton said: "Radicalization and recruitment also is happening online. There's no doubt we have to do a better job contesting online space, including websites and chat rooms, where jihadists communicate with followers. We must deny them virtual territory just as we deny them actual territory. . . . Social media companies can also do their part by swiftly shutting down terrorist accounts so they're not used to plan, provoke, or celebrate violence." *Hillary Clinton on National Security and the Islamic State,* Council on Foreign Relations (Nov. 19, 2015), http://www.cfr.org/radicalization-and-extremism/hillary-clinton-national-security-islamic-state/p37266. President Obama addressed the nation from the Oval Office in early December 2015. According to an article in Politico, a "senior administration official speaking ahead of Obama's speech Sunday told reporters the president's speech would include a discussion about encryption and the social media fight, but the president left that out of the version of the speech that he delivered. (The White House said Monday that the efforts to address this issue are underway.)" Edward-Isaac Dovere, *This Time, Clinton's Closer to the Public Mood than Obama,* Politico (Dec. 8, 2015), http://www.politico.com/story/2015/12/hillary-clinton-obama-national-security-216523. *See also* Nicole Perloth & Mike Isaac, *Terrorists Mock Bids to End Use of Social Media,* N.Y. Times (Dec. 7, 2015) ("As soon as Twitter suspends one account, a new one is created. After the group's 99th account was suspended, it taunted Twitter by creating @IslamicState100, posting images of birthday candles, cake, trophies and fireworks"), http://www.nytimes.com/2015/12/08/technology/terrorists-mock-bids-to-end-use-of-social-media.html; Scott Shane, Matt Apuzzo & Eric Schmitt, *Americans Attracted to ISIS Find an "Echo Chamber" on Social Media,* N.Y. Times (Dec. 8, 2015), http://www.nytimes.com/2015/12/09/us/americans-attracted-to-isis-find-an-echo-chamber-on-social-media.html; Scott Shane, *Internet Firms*

Urged to Limit Work of Anwar al-Awlaki, N.Y. Times (Dec. 18, 2015), http://www.nytimes.com/2015/12/19/us/politics/internet-firms-urged-to-limit-work-of-anwar-al-awlaki.html; Simon Cottee, *The Challenge of Jihadi Cool,* The Atlantic (Dec. 24, 2015), http://www.theatlantic.com/international/archive/2015/12/isis-jihadi-cool/421776; C.J. Chivers, *Behind the Black Flag: The Recruitment of an ISIS Killer,* N.Y. Times (Dec. 20, 2015), http://www.nytimes.com/2015/12/21/world/middleeast/isis-recruitment-killer-hassan-aboud.html?login=email&action=click&pgtype=Homepage&clickSource=story-heading&module=photo-spot-region&region=top-news&WT.nav=top-news.

145 The Office of Personnel Management (OPM) was hacked in 2014, and data on several current and former government employees was taken. *See* Fred Barbash and Ellen Nakashima, *Chinese Hackers May Have Breached the Federal Government's Personnel Office, U.S. Officials Say,* Wash. Post (July 13, 2014), https://www.washingtonpost.com/news/morning-mix/wp/2014/07/09/report-chinese-hacked-into-the-federal-governments-personnel-office.

146 Reuters, *Google: Gmail Hack Likely From China Cyberattackers,* Huffington Post (June 1, 2011), http://www.huffingtonpost.com/2011/06/01/google-gmail-hack-china_n_869995.html.

147 *See, e.g.*, Evan Perez, Tal Kopan and Shimon Prokupecz, *U.S. Investigating Report Email Account Linked to CIA Director Hacked,* CNN (Oct. 20, 2015), http://www.cnn.com/2015/10/19/politics/cia-fbi-alleged-hacking-report/index.html.

148 The question whether the issues discussed in part 3 should be considered as part of FAA renewal, or separately, is one that may depend on legislative tactics and other considerations. I am largely indifferent as to whether these issues are addressed as part of FAA renewal or in a separate process.

The preferred citation for this publication is:
David S. Kris, *Trends and Predictions in Foreign Intelligence Surveillance: The FAA and Beyond,* Hoover Working Group on National Security, Technology, and Law, Series Paper No. 1601 (February 24, 2016), available at http://www.scribd.com/doc/300422389 and at https://www.lawfareblog.com/trends-and-predictions-foreign-intelligence-surveillance-faa-and-beyond.

About the Author

DAVID S. KRIS

David S. Kris is general counsel of Intellectual Ventures. From 2009 to 2011, he was assistant attorney general for national security at the US Department of Justice. From 2003 to 2009 he held various positions at Time Warner, including deputy general counsel and chief ethics and compliance officer. From 1992 to 2003, he was an attorney and then associate deputy attorney general at the Department of Justice. He is the author of several papers on national security and coauthor of the treatise *National Security Investigations and Prosecutions*. He graduated from Harvard Law School in 1991.

Jean Perkins Foundation Working Group on National Security, Technology, and Law

The Working Group on National Security, Technology, and Law brings together national and international specialists with broad interdisciplinary expertise to analyze how technology affects national security and national security law and how governments can use that technology to defend themselves, consistent with constitutional values and the rule of law.

The group focuses on a broad range of interests, from surveillance to counterterrorism to the dramatic impact that rapid technological change—digitalization, computerization, miniaturization, and automaticity—are having on national security and national security law. Topics include cybersecurity, the rise of drones and autonomous weapons systems, and the need for—and dangers of—state surveillance. The working group's output, which includes the Aegis Paper Series, is also published on the *Lawfare* blog channel, "Aegis: Security Policy in Depth," in partnership with the Hoover Institution.

Jack Goldsmith and Benjamin Wittes are the cochairs of the National Security, Technology, and Law Working Group.

For more information about this Hoover Institution Working Group, visit us online at http://www.hoover.org/research-teams/national-security-technology-law-working-group.

Hoover Institution, Stanford University
434 Galvez Mall
Stanford, CA 94305-6003
650-723-1754

Hoover Institution in Washington
The Johnson Center
1399 New York Avenue NW, Suite 500
Washington, DC 20005
202-760-3200

HOOVER INSTITUTION