A TWENTY-FIRST CENTURY FRAMEWORK FOR DIGITAL PRIVACY

WHITE PAPER SERIES

Digital Divergence

DAVID KRIS

NATIONAL CONSTITUTION CENTER

Digital Divergence

By David S. Kris[1]

This paper addresses the effects of digital network technology[2] on statutory and constitutional law. It considers these effects from the perspectives of privacy and security, develops and synthesizes fragmented aspects of the latter perspective, and identifies elements common to both. It argues that advancing technology increases what I refer to as "digital divergence," making it easier for informed and motivated individuals, groups, and governments to defeat surveillance, commit misconduct, and avoid attribution, but harder for everyone else to protect against such misconduct and to control their own personal data. Digital network technology has brought enormous benefits, but digital divergence threatens both privacy and security.

Part I of the paper describes how digital network technology threatens privacy. It summarizes the familiar narrative of how more and more activities generate digital data records, often held by third parties, that are conveniently available for surveillance and analysis by government. The essential elements of this narrative, and its essential prescription for legal change to restore protections for privacy, find their clearest expression in the Supreme Court's decision in *Riley v. California*,[3] which required a warrant to search a smart phone incident to an arrest, and the concurrences of five Justices in *United States v. Jones*,[4] which would require a warrant for any long-term monitoring by technical means of a person's precise location.

Part II describes how digital network technology threatens security. It identifies several factors in the technology that hinder surveillance, and several more that facilitate misconduct. Two of these factors—encryption and cyber threats—have been well publicized, due in part to the FBI's "Going Dark" campaign, but others remain more esoteric and disintegrated. This stems partly from the complex and sometimes classified nature of the security challenges and partly from the diffidence of the U.S. government after Edward Snowden's leaks. Part II attempts to refine and develop the security narrative.

Part III introduces the idea of "digital divergence," a way of understanding and describing how digital network technology simultaneously threatens privacy and security. I use the term "divergence" because digital network technology gives rise to trends that are related to

---

[1] This paper was submitted for prepublication review by the U.S. government on August 30, 2016, cleared, edited and resubmitted in an iterative process over the next several weeks, and last cleared on November 4, 2016. Thanks to Jack Goldsmith and Ben Wittes for helpful comments.

[2] I use "digital network technology" to refer to the familiar technological developments of the last several years, many of them relating to communications—e.g., smartphones and their software applications, the Internet and other packet-switched networks, cloud computing and storage of digital data, GPS, wireless communications protocols such as WiFi and Bluetooth, and related technology.

[3] 134 S. Ct. 2473 (2014).

[4] 132 S. Ct. 945 (2012).

one another and share a common origin, but exert opposite effects. The paper describes four areas of divergence, explaining how digital network technology: (1) creates *more* data of which *less* is relevant; (2) *consolidates* and *fragments* data; (3) has led to *greater* and *lesser* cooperation between government and the private sector; and (4) has increased *freedom of choice*, and hence divergence among individuals, in the use of technology to protect privacy and security. It explains how these trends are eroding both privacy and security.

The impact of digital divergence on statutory and constitutional law, discussed in Part IV, is hard to predict, in part because divergence creates opposing pressures. Legal change favoring privacy could include enhanced warrant requirements for searches of all digital data (including data concerning location and Internet activity) in all settings (including at the border and in the cloud); limits on government's authority to engage in (or compel assistance with) decryption, analysis of previously-collected data, and aerial surveillance; and the elimination of third-party doctrine (under which data conveyed to a third party are no longer private) and of minimization doctrine (under which stricter rules governing the use of acquired data permit broader acquisition of data). Legal change favoring security could include development of substitutes for fragile location-based paradigms regulating surveillance; statutory amendments and new agreements to restore and enhance international access to digital data; increasing expectations or requirements for cooperation between government and the private sector, including with respect to encryption; increased governmental access to metadata and publicly-available data; and perhaps even greater regulation of digital networks.

This paper does not advance specific policy prescriptions, either in favor of privacy or security, but rather *describes* ways of thinking about digital network technology from the perspective of privacy and security, and considers the possible legal and related effects that could result from those ways of thinking. As such, it provides a necessary basis for an informed approach to what some academics refer to as "equilibrium-adjustment" in the digital realm.[5] It similarly supports an informed approach to what the Supreme Court refers to as the need to balance privacy interests against governmental interests to determine what is "reasonable" under the Fourth Amendment.[6]

We are today in the midst of a major equilibrium adjustment, a major rebalancing of privacy and security, due to advances in digital network technology. We seem to understand how the technology threatens privacy, but I think we have not yet understood as well how it threatens security. We need that understanding to find a real equilibrium, to make informed judgments about how best to strike the balance between privacy and security. We need it also to identify technological and legal approaches that may enhance both security and privacy, reversing the trend of the past several years. For that to occur, security advocates need to understand how

---

[5] *See* Orin S. Kerr, *An Equilibrium-Adjustment Theory of the Fourth Amendment*, 125 HARV. L. REV. 476, 487 (2011) (describing "equilibrium-adjustment," the "judicial practice of resolving the hard cases triggered by new facts by determining what rule will best restore the prior equilibrium of police power").

[6] *See, e.g.*, Maryland v. King, 133 S. Ct. 1958, 1970 (2013); United States v. Knights, 534 U.S. 112, 118-119 (2001). As the Court put it in *Jones*, "[a]t bottom, we must assur[e] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted." 134 S. Ct. at 950 (internal quotation omitted); *see id*. at 958 (Alito, J., concurring).

digital network technology threatens privacy, and privacy advocates need to understand how it threatens security. This paper is an effort to increase that understanding.

* * *

I. Digital Network Technology Threatens Privacy

The primary narrative in this field decries the loss of privacy resulting from expanding digital network technology. Its essential elements, familiar to many observers, are as follows:[7]

• More and more human activities, from browsing the Internet to driving through a toll booth, generate enduring digital data records of various types.

• Some of these data can be very revealing—e.g., as to a person's interests or physical location.

• The data may be generated and collected continuously and over long periods of time because digital technology removes many of the logistical challenges associated with long-term surveillance. As Justice Alito explained in his concurring opinion in *Jones*, continuously tracking the location of a horse-drawn coach in 1791 would have required "either a gigantic coach, a very tiny constable, or both—not to mention a constable with incredible fortitude and patience," whereas today a small GPS tracking device attached to the underside of a car will suffice.[8]

• End-users may not even be fully aware of the digital data that are being generated unless they become intimately familiar with the privacy settings and other terms of service for their devices, software applications, and web services.

• In the modern world, there is effectively no escape from this data-generating environment—living off the grid is not feasible.

• The data are often easy to collect because they are conveniently combined in a single device like a smart phone and/or because they are held by third parties such as cloud storage or communications providers (from whom data on multiple end-users may be acquired in bulk).

---

[7] *See, e.g.*, Laura Donohue, *The Fourth Amendment in a Digital World* (forthcoming in NYU Annual Review of American Law (2016)), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2836647; Andrew Pincus, *Evolving Technology and the Fourth Amendment: The Implications of* Riley v. California, CATO SUP. CT. REV. 307 (2014); Andrew Guthrie Ferguson, *Personal Curtilage: Fourth Amendment Security in Public*, 55 WM. & MARY L. REV. 1283 (2014); Adam Lamparello & Charles E. MacLean, Riley v. California: *Privacy Still Matters, But How Much and in What Contexts?*, 27 REGENT U. L. REV. 25 (2014-2015); Alan Butler, *Get a Warrant: The Supreme Court's New Course for Digital Privacy Rights after* Riley v. California, 10 DUKE J. CONST. L. & PUB. POL'Y 83 (2014). *See also* James Urton, *Unearthing Trackers of the Past: UW Computer Scientists Reveal the History of Third-Party Web Tracking* (Aug. 15, 2016), http://www.washington.edu/news/2016/08/15/unearthing-trackers-of-the-past-uw-computer-scientists-reveal-the-history-of-third-party-web-tracking/.

[8] *Jones*, 132 S. Ct. at 958 n.3 (Alito, J., concurring).

• Data not automatically generated for commercial reasons can be specially generated by government targeting (e.g., by installing or activating a vehicle GPS tracking device).

• The collected data are also easy and cheap to store, combine with other information, analyze, and query long after the fact.

This privacy narrative has been effectively advanced by academics, advocacy groups, and communications providers.[9] It has gained significant traction in the Supreme Court, and its proponents imagine fondly a future in which the decision in *Riley*,[10] and the concurrences in *Jones*,[11] have been extended to supply the necessary correction and restore balance,[12] ending the current "golden age"[13] of government surveillance. It is worth reviewing these two cases in some detail, because together they capture most important elements of the privacy narrative concerning digital network technology.

A. The *Riley* Decision

In *Riley*, the Supreme Court held that the police may not, "without a warrant, search digital information on a cell phone seized from an individual who has been arrested."[14] In an opinion by Chief Justice Roberts, the Court rejected the government's argument that "a search of

[9] For academic work, see sources cited *supra* in note 7. For advocacy groups, *see, e.g.*, ACLU, *Privacy and Technology*, https://www.aclu.org/issues/privacy-technology; Electronic Frontier Foundation, *Privacy*, https://www.eff.org/issues/privacy; Jameel Jaffer, *A First Amendment in the Digital Age*—Peter Zenger Lecture (Oct. 4, 2016), https://www.justsecurity.org/33479/a-amendment-digital-age-peter-zenger-lecture/#more-33479. For communications providers, *see, e.g.*, Brad Smith, *Congress Must Update Our Privacy Laws* (Feb. 25, 2016), http://blogs.microsoft.com/on-the-issues/2016/02/25/congress-must-update-our-outdated-privacy-laws/; Ellen Nakashima, *Tech Giants Don't Want Obama to Give Police Access to Encrypted Phone Data*, THE 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 (Apr. 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 (Apr. 28, 2015), http://yahoopolicy.tumblr.com/post/117638169643/usa-freedom-act-time-for-meaningful-government.

[10] 134 S. Ct. 2473 (2014). In *Riley*, the Supreme Court held that the police may not, "without a warrant, search digital information on a cell phone seized from an individual who has been arrested." *Id*. at 2480.

[11] 132 S. Ct. 945 (2012). The Court held that it is a Fourth Amendment search for the police to physically attach a GPS tracking device to a vehicle to monitor its location on public roads, but in two concurring opinions, a total of five Justices made clear that long-term GPS monitoring even without any physical aspect would constitute a search.

[12] *See, e.g.*, Paul Ohm, *The Life of Riley (v. California)*, 48 TEXAS TECH. L. REV. 133 (2015) [hereinafter *Life of Riley*] (providing a roadmap for privacy advocates in the wake of *Riley*).

[13] Peter Swire & Kenesa Ahmad, *'Going Dark' Versus a 'Golden Age for Surveillance'*, CDT (Nov. 28, 2011); Peter Swire, *The Golden Age of Surveillance*, SLATE (July 15, 2015), http://www.slate.com/articles/technology/future_tense/2015/07/encryption_back_doors_aren_t_necessary_we_re_already_in_a_golden_age_of.html.

[14] 134 S. Ct. at 2480.

all data stored on a cell phone is 'materially indistinguishable' from searches of these sorts of physical items [such as paper address books, which have long been allowed incident to an arrest]. That is like saying a ride on horseback is materially indistinguishable from a flight to the moon."[15] The Court relied on several factors for this conclusion, including the "immense storage capacity" of modern smart phones and the many types of data they contain:

> First, a cell phone collects in one place many distinct types of information—an address, a note, a prescription, a bank statement, a video—that reveal much more in combination than any isolated record. Second, a cell phone's capacity allows even just one type of information to convey far more than previously possible. The sum of an individual's private life can be reconstructed through a thousand photographs labeled with dates, locations, and descriptions; the same cannot be said of a photograph or two of loved ones tucked into a wallet. Third, the data on a phone can date back to the purchase of the phone, or even earlier. A person might carry in his pocket a slip of paper reminding him to call Mr. Jones; he would not carry a record of all his communications with Mr. Jones for the past several months, as would routinely be kept on a phone.[16]

The Court also stated that "there is an element of pervasiveness that characterizes cell phones but not physical records. Prior to the digital age, people did not typically carry a cache of sensitive personal information with them as they went about their day. Now it is the person who is not carrying a cell phone, with all that it contains, who is the exception."[17]

The Court in *Riley* emphasized that while "the data stored on a cell phone is distinguished from physical records by quantity alone, certain types of data are also qualitatively different":[18]

> An Internet search and browsing history, for example, can be found on an Internet-enabled phone and could reveal an individual's private interests or concerns—perhaps a search for certain symptoms of disease, coupled with frequent visits to WebMD. Data on a cell phone can also reveal where a person has been. Historic location information is a standard feature on many smart phones and can reconstruct someone's specific movements down to the minute, not only around town but also within a particular building.
>
> In 1926, Learned Hand observed . . . that it is "a totally different thing to search a man's pockets and use against him what they contain, from ransacking his house for everything which may incriminate him." If his pockets contain a cell phone, however, that is no longer true. Indeed, a cell phone search would typically expose to the government far more than the most exhaustive search of a house: A phone not only contains in digital

[15] *Id*. at 2488-89 (citation omitted).

[16] *Id*. at 2489 (footnote omitted).

[17] *Id*. at 2490.

[18] *Id*.

> form many sensitive records previously found in the home; it also contains a broad array of private information never found in a home in any form—unless the phone is.[19]

In short, the Court determined, smartphones have effectively inverted the relative importance to privacy of "effects" and "houses."[20] The fact that "technology now allows an individual to carry such [large and varied amounts of private] information in his hand does not make the information any less worthy of the protection for which the Founders fought."[21]

B. The *Jones* Concurrences

The Supreme Court's decision in *Jones*, issued in 2012, included similar themes expressed in concurring opinions joined by a total of five Justices. The Court in *Jones* held that it is a Fourth Amendment search for the police to physically attach a GPS tracking device to a vehicle to monitor its location on public roads. Justice Scalia's majority opinion focused on the physical trespass involved in placing the tracking device: "It is important to be clear about what occurred in this case: The Government physically occupied private property for the purpose of obtaining information. We have no doubt that such a physical intrusion would have been considered a 'search' within the meaning of the Fourth Amendment when it was adopted."[22]

Justice Alito, joined by three other justices, concurred in the judgment in *Jones*, rejecting the trespass theory: "[T]he Court's reasoning largely disregards what is really important (the use of a GPS for the purpose of long-term tracking) and instead attaches great significance to something that most would view as relatively minor (attaching to the bottom of a car a small, light object that does not interfere in any way with the car's operation)."[23] For Justice Alito, the Court's cases established that "an actual trespass is neither necessary *nor sufficient* to establish a constitutional violation."[24] But long-term collection of GPS information, even without a trespass, was a search:

> [R]elatively short-term monitoring of a person's movements on public streets accords with expectations of privacy that our society has recognized as reasonable. But the use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy. For such offenses, society's expectation has been that law enforcement agents and others would not—and indeed, in the main, simply could not—secretly monitor and catalogue every single movement of an individual's car for a very long period. In this case, for four weeks, law enforcement agents tracked every movement that respondent

[19] *Id*. at 2490-91 (citations omitted).

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

[21] 134 S. Ct. at 2494.

[22] 132 S. Ct. at 949.

[23] *Id*. at 961.

[24] *Id*. at 960 (internal quotation omitted, italics in original).

> made in the vehicle he was driving. We need not identify with precision the point at which the tracking of this vehicle became a search, for the line was surely crossed before the 4-week mark."[25]

Justice Sotomayor also concurred, emphasizing that "the Fourth Amendment is not concerned only with trespassory intrusions on property," and that "even in the absence of a trespass, a Fourth Amendment search occurs when the government violates a subjective expectation of privacy that society recognizes as reasonable."[26] In other words, Justice Sotomayor differed from Justice Alito in concluding that a trespass was sufficient, but not necessary, to create a search. For Justice Sotomayor, several attributes of GPS monitoring, even without a trespass, would "require particular attention" if presented in a future case without the element of physical trespass:

> GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations. The Government can store such records and efficiently mine them for information years into the future. And because GPS monitoring is cheap in comparison to conventional surveillance techniques and, by design, proceeds surreptitiously, it evades the ordinary checks that constrain abusive law enforcement practices: limited police resources and community hostility.[27]

Justice Sotomayor observed that "it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks."[28] Justice Sotomayor's opinion left no real doubt about how she would decide a non-trespassory case of long-term GPS monitoring. Together, *Riley* and *Jones* clearly express all of the key elements of the narrative lamenting the loss of privacy from the rise of digital network technology.

The prescription that follows from the privacy narrative is also reasonably clear: Digital network technology has established a golden age for government surveillance, and something must be done about it. The viable core idea is to remain faithful to the nature of the privacy interests at stake in a search, based on the quantity and quality of the information at issue, even if that means departing from well-established rules developed in the pre-digital era.[29] On that

---

[25] *Id*. at 964 (citations omitted).

[26] *Id*. at 954-55 (internal quotations omitted).

[27] *Id*. at 955-56 (citations and internal quotations omitted).

[28] *Id*. at 957 (citation omitted).

[29] *See, e.g*., Thomas K. Clancy, *Fourth Amendment Satisfaction—The "Reasonableness" of Digital Searches*, 48 TEXAS TECH. L. REV. 37, 38, 61 (2015) (arguing that data searches are governed by the same Fourth Amendment rules regulating containers and document searches, but that the prevalence of the acquisition of digital evidence suggests that traditional, generally applicable rules, though still relevant, need to be rethought and modified); Laura Donohue, *The Fourth Amendment in a Digital World* (forthcoming in NYU ANN. SURV. OF AM. LAW (2016)). Other

approach, *Riley* makes sense because a paper address book or other traditional pocket litter is quantitatively and qualitatively different from a smart phone, even if they all can be carried easily, and *Jones* at least arguably makes sense because uninterrupted GPS surveillance for several weeks is different from most traditional forms of physical surveillance, which is both resource-intensive and challenging to implement seamlessly. Of course, the demise of paper address books and date planners in favor of smart phones means that law enforcement now has access to *less* information than in the past it regularly obtained without a warrant, but if the practical choice is between reducing slightly and increasing dramatically the government's access, *Riley* was correctly decided.[30] The Court's decisions in *Riley* and *Jones*, and associated academic work, advocacy, and commentary have done a good job of explaining the threats to privacy arising from digital network technology and the need for correction.

II. Digital Network Technology Threatens Security

Expanding digital network technology threatens security as well as privacy. But the threat to security has not been as well explained, and is not yet as well understood or accepted, as the threat to privacy, in at least two ways. First, the security threat emerges from several factors, only some of which have received recent attention. Second, those factors have not been as well synthesized into a coherent narrative, and the policy prescriptions that follow therefore have not been as well defined.[31] This part of the paper discusses the ways in which digital network technology threatens security. It identifies five factors that challenge surveillance to detect and prevent misconduct, and four others that facilitate misconduct. Many of these factors are related, however, and more, fewer, or different groupings are possible.

A. Digital Network Factors that Challenge Surveillance Efforts

There are five main factors emerging from technological advances that challenge government's ability to obtain relevant information and intelligence through electronic surveillance. First, there is the increasing international mobility, anonymity, and geographical indeterminacy of persons using and communicating via the Internet and other digital networks.

In the era of landlines, the telephone was the dominant channel for electronic communication; there was only one real U.S. provider (AT&T and its regional subsidiaries); that

---

factors might include the duration of the collection, the use to which the collected information is put, and the number of individuals whose privacy is affected by the collection. *See also* discussion *supra* in note 6.

[30] *Cf. Riley*, 134 S. Ct. at 2497 (Alito, J., concurring) ("Suppose that two suspects are arrested. Suspect number one has in his pocket a monthly bill for his land-line phone, and the bill lists an incriminating call to a long-distance number. He also has in his wallet a few snapshots, and one of these is incriminating. Suspect number two has in his pocket a cell phone, the call log of which shows a call to the same incriminating number. In addition, a number of photos are stored in the memory of the cell phone, and one of these is incriminating. Under established law, the police may seize and examine the phone bill and the snapshots in the wallet without obtaining a warrant, but under the Court's holding today, the information stored in the cell phone is out. While the Court's approach leads to anomalies, I do not see a workable alternative.").

[31] The closest effort has been the FBI's "Going Dark" campaign, but as discussed below that effort has been focused heavily on encryption.

provider had a very cooperative relationship with the U.S. government (in part because it was a regulated monopoly); and a telephone number corresponded to a fixed location and a known subscriber who paid the monthly bill. Since then, the number of channels for electronic communication and the number of providers in each channel has increased dramatically, and some of those providers are not cooperative with the United States government (or are not trusted by the U.S. government to maintain the secrecy of its surveillance targets).[32]

Mobile telephone service has eclipsed fixed-point service,[33] disposable cell phones are readily available, and other forms of mobile communication have also seen vast increases in users—even the now-venerable email account has seen increasing mobile use, such that "[a]nywhere access has become a common feature for all users."[34] Digital networks have allowed advertising-based business models that in turn allow use of these varied communications channels anonymously and without monetary payment.[35] And, of course, international travel, and the options for international travel, have increased dramatically.[36] All this makes it increasingly difficult for government surveillance to find the relevant communications and to determine the location and identity of communicants.

Even when the government finds the right channel and learns what is being said, it may not be able to determine—consistently, reliably, and quickly—who is saying it and where they are.[37] The surveillance targets remain anonymous, in unknown locations, and mobile. As one senior FBI agent has explained:

---

[32] Examples of electronic communications channels include email, chat, IM, SMS, MMS, other messenger services, VOIP, blogs and microblogs (e.g., Twitter), social networks, and online gaming. There are thousands of providers of such services, some of which are based abroad.

[33] The number of children and adults with wireless telephone service only (no landline) has risen from nearly zero in 2003, to nearly 60% for children and nearly 50% for adults as of the end of 2015. Stephen J. Blumberg & Julian V. Luke, *Wireless Substitution: Early Release of Estimates from the National Health Interview Survey, July-December 2015*, CENTERS FOR DISEASE CONTROL (May 2016), http://www.cdc.gov/nchs/data/nhis/earlyrelease/wireless201605.pdf.

[34] The Radicati Group, Inc., *Email Statistical Report 2013-2017*, http://www.radicati.com/wp/wp-content/uploads/2013/04/Email-Statistics-Report-2013-2017-Executive-Summary.pdf ("Social networking will grow from about 3.2 billion accounts in 2013 to over 4.8 billion accounts by the end of 2017 . . . . Anywhere access has become a common feature for all users, who now access their mail from a number of devices, at any time and from any location.").

[35] *See, e.g.*, Google, www.google.com. These providers collect and monetize enormous amounts of digital data. But the data are not as useful to law enforcement and intelligence officials as the relatively pristine information associated with a paid account. Advertising-based economic models existed before the rise of digital network technology, of course, but these were typically in the context of one-to-many, broadcast communications (e.g., over-the-air network television), and even then were sometimes a supplement to models involving a known, paying subscriber at a fixed address (e.g., home delivery of newspapers and magazines).

[36] *See* NSIP § 16:6.

[37] *See, e.g.*, David Kris, *Trends and Predictions in Foreign Intelligence Surveillance* 22-25 (Feb. 25, 2016) [hereinafter *Trends and Predictions*], https://www.lawfareblog.com/trends-and-predictions-foreign-intelligence-surveillance-faa-and-beyond. *See also* Michael Steinbach, FBI Executive Assistant Director, *How Technology Has Transformed the Terrorist Threat Fifteen Years After 9/11* at 2, 6 (referring to "the anonymity of the Internet . . .

> For example, in June 2015 we became aware of an individual known only by an online moniker. This anonymous individual communicated to an overseas terrorist group that planned to conduct an attack in the United States in the coming weeks. But who was it? Male or female? Juvenile or adult? Located in the United States or overseas? Plotting to kill or ready to act? These are questions with answers hidden in an individual's digital footprint. Sometimes the answers are easy to extract, but at other times, they are nearly impossible to find. In this case, the individual provided subtle clues that assisted us in narrowing down the geographic area. This case started like many of our cases today, beginning with an anonymous digital persona, later leading to a physical human being. There is no way to stop the growing identity divide, and technology trends indicate it will only become easier to erect identity barriers to hide a biographic identity. In this case, we resolved to the real person by utilizing a hybrid team consisting of members who had the traditional investigative skills as well as members who had the digital know-how. Without both of these components working in coordination, we would not have been as successful as we were.[38]

Second, there is the increasing international mobility, fragmentation, and geographical indeterminacy of digital data.[39] In 2010, Microsoft opened its first foreign data center in Dublin, Ireland, and it has opened many others in foreign countries since then.[40] Today, Google "stores user data across data centers around the world, with attention on efficiency and security rather than where the data is physically stored. A given email message, for instance, may be stored in several data centers far from the user's location, and an attachment to the message could be stored in several other data centers. The locations of the message, the attachment and copies of

---

Remember, bad guys are actively looking to put as many barriers between their digital and biographic identities as possible by concealing their IP address, using end-to-end encrypted messaging apps, and registering for social media with spoofed identifiers.") [hereinafter Steinbach Talk], http://www.washingtoninstitute.org/uploads/Documents/other/SteinbachStatement20160921-ForDownload.pdf.

[38] Steinbach Talk, *supra* note 37, at 6.

[39] *See, e.g.*, Jennifer Daskal, *The Un-Territoriality of Data*, 125 YALE L. J. 326 (2015), http://www.yalelawjournal.org/article/the-un-territoriality-of-data; *In the Matter of a Warrant to Search a Certain E–Mail Account Controlled and Maintained by Microsoft Corporation*, 2016 WL 3770056 (July 14, 2016); Andrew Woods, *Reactions to the Microsoft Warrant Case* (July 15, 2016), https://www.lawfareblog.com/reactions-microsoft-warrant-case.

[40] *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) (providing Microsoft's explanation for why it stores some users' e-mail in Ireland including the reduction of "network latency" and improving the quality of service for users located closer to Ireland than to the United States).

See also Microsoft, Azure Regions, https://azure.microsoft.com/en-us/regions/; James Fontanella-Khan and Richard Waters, *Microsoft to Shield Foreign Users' Data*, FIN. TIMES (Jan. 22, 2014), http://www.cnbc.com/2014/01/22/microsoft-to-shield-foreign-users-data.html; Janet Kennedy, *Microsoft Dynamics Now Served from Microsoft Cloud in Canada*, Microsoft Press Release (July 10, 2016), https://www.microsoft.com/en-ca/sites/datacentre/default.aspx.

the files may change from day to day."[41] Digital data also transit unpredictably across international packet-switched networks. This creates challenges to security by making it hard for government to know where to look for digital data, by requiring more cumbersome international cooperation to obtain data, and by allowing companies to arbitrage differing legal regimes to block government access to data. For example, as discussed in Part IV, even when a federal judge has found probable cause that stored email contains evidence of a crime, Microsoft today enjoys unilateral authority to prevent U.S. law enforcement from gaining prompt and direct access to that email, simply by moving the email out of the United States—something it can do, more or less, with the touch of a button.[42]

A third problem for security is the increasing availability and use of strong encryption—by default in some applications, and explicitly encouraged by international terrorist groups.[43] As discussed below, encryption is now reasonably well recognized as a problem for surveillance, and hence a threat to security, even if the technical details are not fully understood. Of course, encryption also increases security, by protecting information from hackers, and so its absence would likewise threaten security. The question of the day, currently generating more heat than light, is whether there is a way to allow lawful surveillance of encrypted data without unduly compromising general data security. In an ironic twist, it may be that Apple has inadvertently publicized a solution, but only time will tell.[44] For the foreseeable future, encryption will remain a challenge for lawful surveillance.

Fourth, there is the growth of Fintech, and crypto currencies, which facilitate clandestine payments outside the international banking system. As one commentator has explained, "the law

---

[41] Devlin Barrett & Jay Greene, *U.S. to Allow Foreigners to Serve Warrants on U.S. Firms*, WALL ST. J. (July 15, 2016), http://www.wsj.com/article_email/obama-administration-negotiating-international-data-sharing-agreements-1468619305-lMyQjAxMTA2NjE1NTMxNTUzWj.

[42] This is the law in the Second Circuit based on a lawsuit filed by Microsoft, and would apply to any provider; but it is not necessarily the result that other circuits would reach if the issue were presented to them. The U.S. government has filed a petition for rehearing en banc in the Microsoft case in the Second Circuit, No. 14-2985 (Oct. 13, 2016), https://dlbjbjzgnk95t.cloudfront.net/0851000/851585/microsoft%20rehearing%20.pdf, and has stated publicly that it intends to seek corrective legislation (although it has not yet done so), as discussed further in Part IV. I am aware of no evidence that Microsoft or other major providers have in fact undertaken a policy of data-location arbitrage to defeat surveillance directives from the U.S. government, and Microsoft has called for legislation to address the issue, although it appears to remain committed to some restrictions on U.S. access to data stored abroad. *See* Brad Smith, *Our Search Warrant Case: An Important Decision for People Everywhere* (July 14, 2016), http://blogs.microsoft.com/on-the-issues/2016/07/14/search-warrant-case-important-decision-people-everywhere/.

[43] *See* Sam Schechner & Benoit Faucon, *New Tricks Make ISIS, Once Easily Tracked, a Sophisticated Opponent*, WALL ST. J. (Sept. 11, 2015), http://www.wsj.com/articles/new-tricks-make-isis-once-easily-tracked-a-sophisticated-opponent-1473613106; Margaret Coker, Sam Schechner & Alexis Flynn, *How Islamic State Teaches Tech Savvy to Evade Detection*, WALL ST. J. (Nov. 16, 2015), http://www.wsj.com/articles/islamic-state-teaches-tech-savvy-1447720824. Encryption may support anonymity, but it goes further: Even where the government knows the identity of a communicant, encryption may prevent access to the contents of his or her communications.

[44] *See, e.g.*, Matt Tait, *Apple's Cloud Key Vault and Secure Law Enforcement Access*, LAWFARE (Sept. 14, 2016), https://www.lawfareblog.com/apples-cloud-key-vault-and-secure-law-enforcement-access (discussing the debate over Apple's Cloud Key Vault (CKV) and arguing that CKV as a cryptographic backdoor is a better alternative than government-sponsored hacking).

and policy issues surrounding the bitcoin phenomenon . . . appear to be 'anti-security' impulses—for example, the existence of bitcoin allows for pseudononymous transactions that can obscure malevolent conduct, and that is of concern to law enforcement and intelligence operatives. This anti-security aspect of bitcoin is a natural consequence of the quasi-libertarian, anti-statist nature of the technology."[45] It is a traditional investigative technique to follow the trail of money associated with a crime or other bad event, and to the extent that bitcoin or other Fintech makes that more difficult (even if not impossible), it is a digital technology that challenges security.[46]

Fifth and finally, there is the problem of ever-larger quantities of digital data that may effectively obscure the records of illegal or otherwise dangerous activities.[47] The problem of larger haystacks, or unfavorable signal-to-noise ratios, makes it harder to find the relevant data, and is the main challenge to security in this area. But larger haystacks also require technical and legal innovation—e.g., bulk collection or something like the USA Freedom Act[48]—and compel the creation of larger, more complex governmental systems for filtering, processing, storing, and querying data, which systems will inevitably have more bugs and malfunctions, including both Type I and Type II errors (e.g., both over- and under-collection) as measured against any applicable standard or desired outcome. This is a challenge to security (as well as privacy).

B. Digital Network Factors that Facilitate Misconduct

Apart from the foregoing five factors, which generally make surveillance harder, there are also at least four aspects of digital networks that make misconduct easier.

---

[45] Paul Rosenzweig, *Bitcoin as a National Security Hedge Fund*, LAWFARE (Nov. 6, 2015), https://www.lawfareblog.com/bitcoin-national-security-hedge-fund. Opinions vary on whether Bitcoin is in fact as surveillance-proof as it purports to be. *See, e.g.*, *The Lawfare Podcast: Nick Weaver on Why You Should Sell Your Bitcoin* (Jan. 9, 2016), https://www.lawfareblog.com/lawfare-podcast-nick-weaver-why-you-should-sell-your-bitcoin. But in general the rise of Fintech and crypto currencies allow for financial transactions outside the heavily-regulated banking system in ways that pose challenges for security, and could become untraceable or very difficult to trace as a practical matter even if they are not mathematically immune from surveillance. For a discussion of Fintech and the Internet of Things as issues affecting foreign intelligence surveillance, *see Trends and Predictions*, *supra* note 37, at 25. I am grateful to Todd Hinnen for a recent, helpful discussion of this.

[46] *See, e.g.*, Robert McMillan, *In the Bitcoin Era, Ransomware Attacks Surge*, WALL ST. J. (Aug. 19, 2016), http://www.wsj.com/articles/in-the-bitcoin-era-ransomware-attacks-surge-1471616632; Brett Nigh & C. Alden Pelker, *Virtual Currency: Investigative Challenges and Opportunities* (Sept. 28, 2015), https://leb.fbi.gov/2015/september/virtual-currency-investigative-challenges-and-opportunities.

[47] *See, e.g.*, Techdirt, *The Problem With Too Much Data: Mistaking The Signal For The Noise* (Sept. 10, 2013), https://www.techdirt.com/articles/20130909/12361124455/problem-with-too-much-data-mistaking-signal-noise.shtml; Steinbach Talk, *supra* note 37, at 4 (describing the difficulties of having to "sort through the large volume of social media connections (the noise) to find the digital profiles (the signal) that are part of our terror network. . . . Think how that compares to the historical volume in identifying physical global networks.").

[48] For a discussion of bulk metadata collection, *see* David Kris, *On the Bulk Collection of Tangible Things*, http://jnslp.com/wp-content/uploads/2014/05/On-the-Bulk-Collection-of-Tangible-Things.pdf. For a discussion of the USA Freedom Act, *see* NSIP Chapter 19.

First, fraud, theft, espionage, sabotage, terrorism, attacks, and covert action, and influence are all possible on a much greater (and faster) scale in cyberspace than in the physical world, and without regard to location (of either the perpetrator or victim of misconduct). The cyber threat has been well publicized,[49] including the relatively recent focus on cyber influence through the theft and public release of emails from the Democratic National Committee,[50] and possible foreign hacking of state voting systems.[51] The evolving nature of the cyber threat with respect to information—from secretly stealing, to stealing and publishing, to manipulating without stealing—may not be fully appreciated or integrated into policy, but in general the cyber threat is acknowledged.

Related to this is a second factor, albeit less widely publicized: The growing number of (private, and often covert) communications channels and illicit online marketplaces, including the Dark Web, which facilitates nefarious public-private partnerships, lowers barriers to entry into high-level cyber misconduct, and hinders attribution of that misconduct.[52]

Third, by reducing the significance of physical location, technology has also increased the significance of the growing number of failed states and ungoverned areas all over the world. Using digital networks, bad actors in such areas can produce effects, including kinetic effects, everywhere, including in the United States.[53] More generally, by reducing the significance of physical location, digital network technology reduces the defensive significance of geography and increases the number of targets available to any bad actor, and the number of bad actors who can strike any target.[54] For example, digitally networked industrial "SCADA" systems are

---

[49] *See, e.g.*, John Carlin, *Detect, Disrupt, Deter: A Whole-of-Government Approach to National Security Cyber Threats*, http://harvardnsj.org/wp-content/uploads/2016/06/Carlin-FINAL.pdf.

[50] *See, e.g.*, Paul Rosenzweig, *More DNC Leaks*, LAWFARE (Aug. 13, 2016), https://www.lawfareblog.com/more-dnc-leaks.

[51] *See, e.g.*, Joint DHS and ODNI Election Security Statement (Oct. 7, 2016) ("The U.S. Intelligence Community (USIC) is confident that the Russian Government directed the recent compromises of e-mails from US persons and institutions, including from US political organizations . . . . intended to interfere with the US election process"); Ellen Nakashima, *Russian Hackers Targeted Arizona Election System*, THE WASH. POST (Aug. 29, 2016), https://www.washingtonpost.com/world/national-security/fbi-is-investigating-foreign-hacks-of-state-election-systems/2016/08/29/6e758ff4-6e00-11e6-8365-b19e428a975e_story.html.

[52] *See, e.g.*, *Shedding Light on the Dark Web*, THE ECONOMIST (July 16, 2016), http://www.economist.com/news/international/21702176-drug-trade-moving-street-online-cryptomarkets-forced-compete. *See also* discussion of cooperation between governments and the private sector *infra* in note 87.

[53] *See, e.g.*, *The Lawfare Podcast: John Brennan on "Emerging Challenges,"* LAWFARE (Aug. 6, 2016), https://www.lawfareblog.com/lawfare-podcast-john-brennan-emerging-challenges.

[54] *See* Remarks of Director James Comey, *The FBI's Approach to the Cyber Threat* ("The challenge we face today, with a threat that comes at us at the speed of light from anywhere in the world, is that physical place isn't such a meaningful way to assign work any longer.") (Aug. 30, 2016), https://www.fbi.gov/news/speeches/the-fbis-approach-to-the-cyber-threat. *See also* Jack Goldsmith, *The New Vulnerability*, THE NEW REPUBLIC (June 6, 2010) https://newrepublic.com/article/75262/the-new-vulnerability.

enormously convenient and helpful in many ways, but they are also more vulnerable to more attacks by more attackers than traditional control systems.[55]

Finally, the rise of digital networks has helped dangerous and criminal enterprises in many of the same ways that it has helped legitimate businesses, by expanding reach and creating efficiencies. Perhaps chief among these benefits is in propaganda and recruitment, with ISIL's recent online efforts being particularly notable.[56] To be sure, law enforcement and security organizations have also benefited in their own operations—*e.g.*, some DOJ attorneys and FBI personnel recently gained the ability to send unclassified email on iPhones, and the FBI recently released a bank robbery application[57]—but the effects are asymmetric, in the sense that modern technology (including but not limited to digital network technology) has generally increased and democratized destructive power more than preventive and remedial capabilities.[58] As destructive power grows, particularly in the digital realm, offense becomes easier than defense.

---

[55] SCADA stands for Supervisory Control and Data Acquisition, and is a system used to control large, industrial processes, often over networks. SCADA systems may eliminate the need for a human being to monitor those processes in real time and space, allowing sensors to trigger warnings that go to remote observers, but they also may allow for nefarious manipulation of the processes from afar. *See, e.g.*, IDAHO NAT'L LABS., U.S. DEP'T OF ENERGY, VULNERABILITY ANALYSIS OF ENERGY DELIVERY CONTROL SYSTEMS, (2011), http://energy.gov/sites/prod/files/Vulnerability%20Analysis%20of%20Energy%20Delivery%20Control%20Systems%202011.pdf ("Cybersecurity for energy delivery systems has emerged as one of the Nation's most serious grid modernization and infrastructure protection issues.. . . A key part of the program is SCADA system vulnerability analysis that identifies and provides mitigation approaches for vulnerabilities that could put these systems at risk.").

[56] *See, e.g.*, Michael Steinbach, Executive Assistant Director, FBI, *ISIL Online: Countering Terrorist Radicalization and Recruitment on the Internet and Social Media* (July 6, 2016), https://www.fbi.gov/news/testimony/isil-online-countering-terrorist-radicalization-and-recruitment-on-the-internet-and-social-media-. Before his death, Anwar Awlaki was also a powerful recruiter of terrorists using the Internet, although his online efforts had lower production values than ISIL's current work, and used more traditional broadcast models, such as spreading his sermons via the Internet. *See, e.g.*, Scott Shane & Souad Mekhennet, *Imam's Path From Condemning Terror to Preaching Jihad*, NY TIMES (May 8, 2010), http://www.nytimes.com/2010/05/09/world/09awlaki.html; *see also* Steinbach Talk, *supra* note 37, at 2.

As reported by one CIA historian, ISIL's online propaganda has an interesting analogue in the development and use of short-wave radio prior to World War II by sponsors of competing ideologies in Europe and Asia to propagandize and subvert. *See* Joseph E. Roop, *Foreign Broadcast Information Service, History, Part I: 1941-1947* 3 (1969), https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/foreign-broadcast-information-service/.

[57] *See* FBI Releases New Bank Robbers Mobile App (Aug. 19, 2016), https://www.fbi.gov/news/stories/fbi-releases-new-bank-robbers-mobile-app; *see also* Alfred Ng, *This is NYPD's Official Crime-Fighting Phone*, CNET (Oct. 13, 2016), https://www.cnet.com/news/nypd-new-york-police-official-crime-fighting-windows-phone/.

[58] *See, e.g.*, Nathan Myhrvold, *Strategic Terrorism: A Call to Action* (July 13, 2013), https://www.lawfareblog.com/nathan-myhrvold-strategic-terrorism-call-action-lawfare-research-paper-series; David E. Sanger, *Cyberthreat Posed by China and Iran Confounds White House*, NY TIMES (Sept. 5, 2015) ("'Offense is moving a lot faster than defense,' Mr. Obama told troops on Friday at Fort Meade, Md., home of the National Security Agency and the United States Cyber Command"), http://www.nytimes.com/2015/09/16/world/asia/cyberthreat-posed-by-china-and-iran-confounds-white-house.html. *See also* Goldsmith, *The New Vulnerability*, *supra* note 54 ("Both cyber attacks and cyber exploitations are very hard to defend against. 'The aggressor has to find only one crucial weakness; the defender has to find all of them, and in advance,' wrote Herman Kahn in 1960 in his famous book *On Thermonuclear War*. This generally true proposition about defense systems has special salience for computer networks.").

Two of these threats to security—cyber-threats and encryption—have been well publicized,[59] but in general the security narrative has not been as well understood, coherently developed, or widely accepted as the privacy narrative.[60] To be sure, the FBI has argued that new technology creates a risk of "Going Dark," which could in theory expand to address many of the challenges to surveillance discussed above. But most versions of "Going Dark," especially recently, have focused on encryption.[61]And even those narrower arguments have not been widely accepted.[62] That is likely the case for several reasons, including the highly technical (and in some cases, classified) nature of the challenges and the policy preferences at the highest levels of the Executive Branch (the default champion for security) in the aftermath of the Snowden disclosures.[63] As Cameron Kerry, former General Counsel of the Department of Commerce, has

[59] *See, e.g.*, John Carlin, *Detect, Disrupt, Deter: A Whole-of-Government Approach to National Security Cyber Threats*, http://harvardnsj.org/wp-content/uploads/2016/06/Carlin-FINAL.pdf; James Comey, Testimony Before the House Judiciary Committee, *Encryption Tightrope, Balancing Americans' Security and Privacy* (Mar. 1, 2016), https://www.fbi.gov/news/testimony/encryption-tightrope-balancing-americans-security-and-privacy; Steinbach Talk, *supra* note 37, at 3 ("Very few of our targets are communicating in the open today.").

[60] *See, e.g.*, 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.

[61] *See* Remarks of Director James Comey, *The FBI's Approach to the Cyber Threat* (Aug. 30, 2016), https://www.fbi.gov/news/speeches/the-fbis-approach-to-the-cyber-threat ("I can't get on the stage without talking a little bit about the problem we call Going Dark, which is encryption.") Early versions of "Going Dark" arguments focused on live interception rather than stored data, and did not emphasize problems with encryption, but more recent versions have done both, and also emphasized the dangers of social media. *Compare, e.g.*, Valerie Caproni, Statement Before the House Judiciary Committee, Subcommittee on Crime, Terrorism, and Homeland Security (Feb. 17, 2011), https://archives.fbi.gov/archives/news/testimony/going-dark-lawful-electronic-surveillance-in-the-face-of-new-technologies, *with* FBI, Going Dark, https://www.fbi.gov/services/operational-technology/going-dark, and James Comey, Joint Statement with Deputy Attorney General Sally Quillian Yates Before the Senate Judiciary Committee, *Going Dark: Encryption, Technology, and the Balances Between Public Safety and Privacy* (July 8, 2015), https://www.fbi.gov/news/testimony/going-dark-encryption-technology-and-the-balances-between-public-safety-and-privacy. Recently, the disputes between the FBI and Apple in San Bernardino have increased the focus on encryption to the exclusion of almost all other issues. *See, e.g.*, Matt Apuzo, *F.B.I. Used Hacking Software Decade Before iPhone Fight*, NY TIMES (Apr. 13, 2016), http://www.nytimes.com/2016/04/14/technology/fbi-tried-to-defeat-encryption-10-years-ago-files-show.html. A notable recent exception is Michael Steinbach's September 21, 2016 talk at the Washington Institute, given after this paper was submitted to the government for prepublication review, which does attempt a more comprehensive assessment of technology's effects on security, discussing anonymity on the Internet, encryption, and the increasing volume of information, among other factors. *See* Steinbach Talk, *supra* note 37.

[62] *See, e.g.*, *Don't Panic: Making Progress in the "Going Dark" Debate*, Berkman Center, Harvard University (Feb. 1, 2016), https://cyber.law.harvard.edu/pubrelease/dont-panic/; *see also* The Chertoff Group, *The Ground Truth About Encryption* (2016), https://chertoffgroup.com/cms-assets/documents/238024-282765.groundtruth.pdf.

[63] *See, e.g.*, Benjamin Wittes, *The Obama Administration's Encryption Wrangling*, LAWFARE (Sept. 8, 2015), https://www.lawfareblog.com/obama-administrations-encryption-wrangling (referring to a National Security Council options paper on encryption that was leaked to the *Washington Post* and that "lays out three options for the administration—three options that notably do not include seeking legislation on encryption." As reported in the NSC document, the options are: 1) "Disavow Legislation and Other Compulsory Actions"; 2) "Defer on Legislation and Other Compulsory Actions"; and 3) "Remain Undecided on Legislation or Other Compulsory Actions.") Wittes concludes: "it probably doesn't matter all that much which of these options Obama chooses. If these are the choices on the table, industry has already won." *But see* Michael D. Shear, *Obama, at South by Southwest, Calls for Law*

explained, after those disclosures, the Obama Administration, through the National Security Council, made a decision to shift policy-making power away from traditional national security agencies and towards commerce-oriented agencies and private sector companies (such as communications providers).[64] And they, in turn, "push[ed] for a stronger message on privacy while dialing back the emphasis on security."[65] Whether this is good or bad policy, it is certainly significant, and represents a major change in the inter-agency balance of power that has existed since at least September 11, 2001 (and perhaps for much longer). It will be interesting to see whether there is pent-up demand for recognition and development of the security narrative and its prescription for legal change, latent in federal law enforcement and the U.S. Intelligence Community, that finds expression in the beginnings of a new presidential administration.

III. Digital Divergence

Although there is much disagreement about the policy prescriptions that follow, it is reasonably clear that both of the foregoing narratives are factually correct: While changing technology has brought incredible benefits, it threatens both privacy and security.[66] That unfortunate situation challenges the traditional view of privacy and security as being locked in a zero-sum game, where one value's gain must be the other's loss, and the only question is how to strike the balance between them. How can *both* values be declining as digital network technology advances?

This part of the paper argues that privacy and security are both declining due to "digital divergence." That is, digital network technology has produced at least four pairs of divergent trends—i.e., trends that are related to one another, and share a common origin in the technology, but exert opposite effects. These pairs of opposite trends are in some ways like the two sides of a

---

Enforcement Access in Encryption Fight, NY TIMES (Mar. 11, 2016), http://www.nytimes.com/2016/03/12/us/politics/obama-heads-to-south-by-southwest-festival-to-talk-about-technology.html. (Of course, these remarks do not establish that NSC leadership is acting *ultra vires*.)

[64] Kerry explains that "the landscape is different" in the government in 2016 than it was until 2013, as the Obama administration learned from the experience of managing the Snowden disclosures and has since "taken numerous steps to restore trust and integrate a broader outlook into its policymaking in the digital arena," as well as expanding and empowering its technology staff and involving them, and other agencies, in national security decisionmaking. Cameron Kerry, *Bridging the Internet-Cyber Gap: An Overview* (Oct. 7, 2016), https://www.lawfareblog.com/bridging-internet-cyber-gap-overview. *See also* Cameron Kerry, *Bridging the Internet-Cyber Gap: Digital Policy Lessons for the Next Administration* (Oct. 2016), https://www.brookings.edu/wp-content/uploads/2016/10/internet-cyber-gap-final.pdf.

[65] Cameron Kerry, *Bridging the Internet-Cyber Gap, supra* note 64.

[66] Digital network technology also may *protect* privacy in certain important ways. *See, e.g.*, Ben Wittes & Jodie Liu, *The Privacy Paradox: The Privacy Benefits of Privacy Threats*, https://www.brookings.edu/wp-content/uploads/2016/06/Wittes-and-Liu_Privacy-paradox_v10.pdf (arguing that digital network technology advances privacy by eliminating the need for potentially embarrassing personal interactions involved in commerce, research, and consumption of information—*e.g.*, online purchases have replaced in-person purchases of pornography or condoms from a drugstore clerk, online research has replaced in-person research into medical conditions with the aid of a librarian, and riding the subway reading *50 Shades of Grey* on a Kindle has replaced reading a paperback edition the cover of which is visible to other riders.").

coin, but they are not static, and indeed are becoming more pronounced over time. This is divergence as the dictionary defines it—"a drawing apart (as of lines extending from a common center)."[67] Here are the four pairs of divergent trends:

• Digital network technology creates *more* private data of which *less* is relevant to security. All other things being equal, more private data is bad for privacy, but more irrelevant data—data pertaining to innocent persons—is bad for security because of the haystack effect and other factors.

• Digital network technology encourages both *consolidation* and *fragmentation* of data. Consolidation permits wholesale compromise of privacy, as the Court recognized in *Riley* and as commercial companies' data breaches regularly confirm, but fragmentation of data does not reliably protect privacy in part because of challenges in systematically safeguarding fragmented data from opportunistic compromise.

• Digital network technology has led to *greater* and *lesser* cooperation among governments, and between government and the private sector. Western governments have not advanced their formal data-sharing relationships beyond Mutual Legal Assistance Treaties (MLATs), which are valuable but insufficient in a digitally networked world. Some of the most cooperative emerging public-private partnerships are between adversarial foreign governments and black-hat hackers, while U.S. communications providers are generally reducing their cooperation with the U.S. government (which may promote privacy but may also reduce security).

• Above all, digital network technology has allowed greater *freedom of choice* in the way that end users protect their data privacy.[68] Unfortunately, some of the persons and entities representing the most significant security threats may be among those most willing and able to employ protective measures, while on average the innocent masses may tend to leave themselves exposed.[69]

In the digital realm, privacy depends largely on control over digital data—i.e., the ability of individuals to understand and determine what data concerning them (to, from, or about them) are generated, retained, revealed, acquired by others, and used or manipulated. Correspondingly,

---

[67] *Divergence*, MERRIAM-WEBSTER DICTIONARY (2016), http://www.merriam-webster.com/dictionary/divergence. In more philosophical terms, the effects could also be described as antinomies. *See, e.g.*, Immanuel Kant, *Critique of Pure Reason* 328 (Norman Kemp Smith trans., 1929); Immanuel Kant, *Prolegomena to Any Future Metaphysics* 337-340 (Acad. Ed. pagination). I am indebted to Jack Goldsmith for suggesting the use of antinomies.

[68] There is an argument that encryption by default, rather than by active user choice, poses a problem for security. There is some truth to this. But there is also the higher-level choice between channels that encrypt by default and those that do not. The basic point I am making is that where there is a choice, bad actors may be more willing and able than good ones to make a choice to control and conceal their data.

[69] These four pairs of trends, like some of the factors identified in Part II, are related to one another in certain ways, and it is certainly possible to imagine more, fewer, or different pairings. In particular, the first two pairs—more/less data and consolidated/fragmented data—are focused on how data exist in the digital realm. The second two pairs—more/less cooperation and freedom of choice—are more focused on human reactions to digital network technology.

security is threatened by the privacy of those who threaten it—their ability to control digital data concerning themselves and their misconduct makes it harder to detect, disrupt, deter, and defend against that misconduct.[70] Digital divergence reveals trends generally favoring control of data by bad actors more than by good ones.

A. More Data of Which Less is Relevant

While digital network technology helps generate far *more data*, all of which is theoretically available to government, far *less data* (a tiny percentage of the growing whole) is pertinent to law enforcement or intelligence, and the most pertinent data may be the *hardest to obtain*. As to the growing amount of digital data, Justice Sotomayor's concurrence in *Jones*, discussed in Part I, correctly notes that in "the digital age . . . people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks,"[71] and that much of this data is stored and thus potentially available for collection. Some estimates have approximately 200 billion email messages being sent daily, with other forms of digital communications growing faster.[72] There is a huge and expanding amount of personal, digital data retained in the world.[73] All other things being equal, this is bad for privacy (regardless of whether it creates other benefits, such as convenience or efficiency).

On the other hand, the existence of more private data is not always good for security, because the vast majority of it is irrelevant to security. To be sure, when security officials find a lawful surveillance target they may be able to acquire a lot of information about him, but the enormous digital haystacks make it harder for them to know where to look, and how to find, the most relevant targets and information. Today, digital data move stochastically, driven by economic and technical variables in a complex and very large mix.[74] Moreover, as discussed in

[70] Of course, privacy in general includes more than control over personal data, and security threats in general arise from more than the data privacy of bad actors. As they pertain to digital network technology, however, privacy at a minimum depends heavily on control of digital data, and such control by malefactors at a minimum contributes heavily to the threats they pose.

[71] 132 S. Ct. at 957.

[72] The Radicati Group, Inc., *Email Statistical Report 2013-2017*, http://www.radicati.com/wp/wp-content/uploads/2013/04/Email-Statistics-Report-2013-2017-Executive-Summary.pdf.

[73] According to Cisco, "mobile data traffic "reached 3.7 exabytes per month at the end of 2015, up from 2.1 exabytes per month at the end of 2014," has "grown 4,000-fold over the past 10 years and almost 400-million-fold over the past 15 years"; "mobile devices and connections in 2015 grew to 7.9 billion, up from 7.3 billion in 2014." Cisco expects monthly data traffic to be "30.6 exabytes by 2020." *See Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2015–2020 White Paper* (Feb. 1, 2016) [hereinafter Cisco Mobile Report], http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/mobile-white-paper-c11-520862.html. In 2011, academic researchers found that "humankind is able to store at least 295 exabytes of information," and that capacity has surely grown enormously since then. Suzanne Wu, *How Much Information Is There in the World?*, USC NEWS (Feb. 10, 2011), http://news.usc.edu/29360/how-much-information-is-there-in-the-world/.

[74] A circuit-switched network, of the sort used by old-fashioned telephone service, involves a dedicated circuit established between two endpoints. In a packet-switched network, data is broken into packets and each packet may be routed on a different path across networks before coming together at the endpoints. As such, packet-switched networks often intermingle various forms of data from multiple communicants. *See* DAVID S. KRIS & J. DOUGLAS

Part II, the most relevant data may be disguised or shielded, making them even harder to discern. In short, more aspects of more lives may be recorded in digital form, but it may be harder for security officials to find the signal in the growing noise, especially if it is encrypted, anonymized, run through a proxy server, and hiding in the shadows of the Dark Web.[75]

B. Consolidation and Fragmentation of Data

Digital network technology has had both a *consolidating* and a *fragmenting* effect on data. The Supreme Court recognized the consolidating effect in *Riley*, noting that smartphones have enormous storage capacities and contain many and varied forms of personal information.[76] Cloud storage sites are arguably even more consolidated, as they may contain enormous quantities of different types of data, sometimes from many different individuals or businesses, as recognized in the discussion of third-party doctrine in Justice Sotomayor's concurrence in *Jones*.[77]

The fragmenting effect emerges from the increasing mobility and anonymity of people and data, as discussed in Part II, and at least three related trends:

- There has been a shift in emphasis away from one-to-many communications models (e.g., broadcast television, radio, newspapers, magazines) towards one-to-few or one-to-one models (e.g., email, IM, chat, SMS, MMS).

- There has been a shift from unilateral communications, in which the audience does not directly interact with the broadcaster (or does so only much later and in limited form, through something like a letter to the editor), to fully interactive, bilateral, or multilateral communications conducted in real time (e.g., a social media news feed with comments).

- Most importantly, there has been a shift from a tiny number of one-to-one communications providers and types (e.g., AT&T telephones) to a huge number of both (e.g., proliferating telephone, email, message, and other communications types with multiple providers for each type).

These developments have occurred not only domestically within the United States, but internationally, with individuals traveling widely, and their digital data increasingly in use, in transit, and in storage all over the world.

WILSON, NATIONAL SECURITY INVESTIGATIONS AND PROSECUTIONS (2d ed. 2012) [hereinafter *NSIP*] §§ 6:11 & n.5, 7:17 & n.2, 7:25, 16:6 & n.6.

[75] *See, e.g.*, Techdirt, *The Problem With Too Much Data: Mistaking The Signal For The Noise* (Sept. 10, 2013), https://www.techdirt.com/articles/20130909/12361124455/problem-with-too-much-data-mistaking-signal-noise.shtml.

[76] 134 S. Ct. at 2491 ("a cell phone search would typically expose to the government far more than the most exhaustive search of a house").

[77] 132 S. Ct. at 957.

In general, consolidation of data threatens privacy in the same way as does the creation of more data. More private information exists, and because it is consolidated it may be more easily acquired. All other things being equal, this is bad for privacy, as the Court recognized in *Riley*. With respect to third-party consolidators, including but not limited to cloud providers, this trend is even more pronounced: When large retailers are hacked, for example, it threatens the privacy of all of their tens of millions of customers at once.[78] (Of course, some hacks threaten both privacy and security, as shown by the successful cyber-theft from OPM, which gave the Chinese government access to the most intimate PII of millions of U.S. government officials who have access to classified information.[79])

On the other hand, consolidation of data may also promote security in a way that the creation of more (irrelevant) data does not. That is because the relevant data, being consolidated, may be easier to find and acquire (lawfully), even if they are surrounded by a lot of chaff. To be sure, however, that is not always the case: Consolidation may make it harder to collect data because it increases the incentive to protect data (e.g., using encryption), while fragmentation may have the opposite effect for most individual users, especially those with scattered data, who are not sophisticated or motivated enough to do so systematically across all of the many platforms on which their data may transit or reside.[80] But as a general matter, particularly with respect to third-party consolidators (e.g., cloud providers) who often hold data that is mirrored locally on end users' devices, consolidation promotes security by making it easier for the U.S. government to find and collect data lawfully, even as it also threatens privacy by allowing others to do so unlawfully. To take the most obvious example, FISA and Title III wiretaps are typically implemented through communications providers, not by direct, physical access to end users' devices.

Fragmentation generally exerts the opposite effects: It tends to make data harder to find and collect, and may therefore promote privacy through a generalized haystack effect. But it doesn't promote privacy in a way that should inspire confidence or comfort, because it leaves end users open both to opportunistic threats, such as drift-net phishing, as well as more targeted efforts, not restrained by law, to collect private information by hacking a personal email account (as famously happened to the Director of the CIA and other officials).[81] On the other hand,

---

[78] *See, e.g.*, Elizabeth A. Harris & Nicole Perlroth, *For Target, the Breach Numbers Grow*, NY TIMES (Jan. 10, 2014), http://www.nytimes.com/2014/01/11/business/target-breach-affected-70-million-customers.html.

[79] *See* Mike Levine and Jack Date, *22 Million Affected by OPM Hack, Officials Say*, ABC News (July 9, 2015), http://abcnews.go.com/US/exclusive-25-million-affected-opm-hack-sources/story?id=32332731.

[80] *See, e.g.*, Dropbox, *How Secure is Dropbox*, https://www.dropbox.com/help/27. By contrast, some individual end users may have very sensitive personal data stored on unencrypted hard drives in their laptop computers.

[81] *See* Devlin Barrett, *FBI Arrests Two in String of Breaches at CIA*, Justice Department, WALL ST. J. (Sept. 8, 2016), http://www.wsj.com/articles/fbi-arrests-two-in-string-of-breaches-at-cia-justice-department-1473354725; 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; Amy Chozick, *John Podesta Says Russian Spies Hacked His Emails to Sway Election*, NY TIMES (Oct. 6, 2016), http://www.nytimes.com/2016/10/12/us/politics/hillary-clinton-emails-wikileaks.html?login=email&_r=1 ; Dan Zak, *A Portrait of John Podesta, Based Entirely on His Hacked Emails*, THE WASH. POST (Oct. 20, 2016),

fragmentation does tend to challenge surveillance that is both targeted (or at least focused on data that are relevant to a legitimate law enforcement and national security mission) and restrained by law.[82] As in the case of the trend towards more/less data, a key problem with respect to consolidated/fragmented data, that makes the equation asymmetric, is that everyone has data that are private, but only a few have data that are relevant to security.

C. Effects on Government Cooperation

Recently, *cooperation* among governments and between the private sector and government, which is essential in protecting both privacy and security, has been simultaneously *increasing* and *decreasing*. The need for greater cooperation between governments rises as people and data increasingly move, come to rest, and exert effects across international and other geographical boundaries, as discussed above. The need for cooperation between governments and the private sector arises because so much of the Internet (particularly the Internet backbone) is owned and operated by the private sector,[83] because so much user data is held by the private sector, and because so much of the digital technology that affects privacy and security (e.g., encryption, social networking, and messaging applications) is developed and maintained by the private sector.[84] Where governments do not cooperate with one another, and where the private sector does not cooperate with governments, data will tend to remain more inaccessible to intelligence and law enforcement officials.

Today, the U.S. government has not been able to advance beyond a Mutual Legal Assistance Treaty (MLAT) even with its closest ally, the UK, as discussed in Part II. A broader, multi-lateral agreement with other allies is even more remote. At the same time, major U.S. communications companies are *decreasing cooperation* with the U.S. government, while purveyors of malware and cyber tools are *increasing cooperation* with certain foreign governments. These differing private-sector attitudes may not stem unavoidably from increasing digital network technology, but that technology certainly enabled them. Edward Snowden's disclosures probably would not have been possible without digital network technology that allowed him to exfiltrate huge amounts of classified data from NSA's networks (had he attempted to print and remove the data on paper in the same amount of time, he likely would

---

https://www.washingtonpost.com/lifestyle/style/a-portrait-of-john-podesta-based-entirely-on-his-hacked-emails/2016/10/20/63655b26-96cd-11e6-bb29-bf2701dbe0a3_story.html.

[82] Bulk collection of metadata, which was lawful and not targeted, is arguably a counter-example, but even that collection was subject to strict limits on the use of the data. *See* discussion *infra* at text and note 141.

[83] *See, e.g.*, Jonathan Strickland, *Who Owns the Internet*, http://computer.howstuffworks.com/internet/basics/who-owns-internet1.htm.

[84] For example, one of the reasons the British government is so keen to have access directly to U.S. communications providers is that the increased use of encryption and other technologies has increased its dependence on those providers for provision of clear text. *See Trends and Predictions*, *supra* note 37, at 20-22; David Kris, *Preliminary Thoughts on Cross-Border Data Requests*, LAWFARE (Sept. 28, 2015) [hereinafter *Cross-Border Data Requests*], https://www.lawfareblog.com/preliminary-thoughts-cross-border-data-requests.

have aroused suspicion).[85] Faced with shifting public opinion resulting from those disclosures and the Obama Administration's response to them, communications companies reduced their cooperation with the U.S. government mainly to bolster international and domestic customer confidence in their digital network and cloud offerings.[86] And the growing number of public-private marketplaces for hacking tools and zero-day exploits, as well as the market for protection against such threats, owe both their existence and their wares to digital network technology.[87]

[85] According to the House Intelligence Committee, Snowden took 1.5 million documents from NSA. Executive Summary of Review of the Unauthorized Disclosures of Former National Security Agency Contractor Edward Snowden 1-2 (Sept. 15, 2016), http://intelligence.house.gov/uploadedfiles/hpsci_snowden_review_-_unclass_summary_-_final.pdf.

[86] For a description of the fact of reduction in cooperation, *see Trends and Predictions*, *supra* note 37, at 20-21 & n.115. For an explanation of why the providers have reduced cooperation, *see, e.g.*, Brad Smith, *Unfinished Business on Government Surveillance Reform* (June 4, 2014), http://blogs.microsoft.com/on-the-issues/2014/06/04/unfinished-business-on-government-surveillance-reform. It is important to be clear about the reduction in cooperation by U.S. providers. They have not engaged in general civil disobedience; rather, they have challenged production orders in court. There is, of course, no legitimate security interest in permitting unlawful U.S. governmental access to data, any more than there is a legitimate privacy interest in blocking lawful access. Nor have the providers raised frivolous legal arguments (Microsoft prevailed in the Second Circuit, as discussed in Part II). Nor, as far as I know, have they attempted to engage in what might be called data-location arbitrage, moving all of their customers' email accounts offshore in an effort to put them beyond the reach of the Stored Communications Act. *See also* discussion in note 42, *supra*.

[87] Governments are reported to buy hacking tools and other malware from private individuals or companies, essentially digital arms dealers. *See, e.g.*, Andy Greenberg, *New Dark-Web Market is Selling Zero-Day Exploits to Hackers*, Wired (Apr. 17, 2015), https://www.wired.com/2015/04/therealdeal-zero-day-exploits/; Nicole Perloth, *iPhone Users Urged to Update Software After Security Flaws are Found*, NY TIMES (Aug. 25, 2016), http://www.nytimes.com/2016/08/26/technology/apple-software-vulnerability-ios-patch.html; Nicole Perlroth & David E. Sanger, *Nations Buying as Hackers Sell Flaws in Computer Code*, NY TIMES (July 13, 2013), http://www.nytimes.com/2013/07/14/world/europe/nations-buying-as-hackers-sell-computer-flaws.html?_r=0; Nicholas Weaver, *NSA and the No Good, Very Bad Monday*, LAWFARE (Aug. 16, 2016), https://www.lawfareblog.com/very-bad-monday-nsa-0. It is clear that various governments and the private sector are increasingly cooperating in this area.

The market for protection against digital network threats also admits of synergies between government and the private sector. *See, e.g.*, Corey Flintoff, *Kaspersky Lab: Based In Russia, Doing Cybersecurity In The West*, NPR (Aug. 10, 2015), http://www.npr.org/sections/alltechconsidered/2015/08/10/431247980/kaspersky-lab-a-cybersecurity-leader-with-ties-to-russian-govt. In August 2016, Kaspersky and Symantec revealed what the latter referred to as "cyberespionage-style attacks against selected targets in Russia, China, Sweden, and Belgium" by a "group called Strider." Symantec: *Strider: Cyberespionage Group Turns Eye of Sauron on Targets* (Aug. 7, 2016), *available* at http://www.symantec.com/connect/blogs/strider-cyberespionage-group-turns-eye-sauron-targets; *see also* Kaspersky, *ProjectSauron: Top Level Cyber-Espionage Platform Covertly Extracts Encrypted Government Comms* (Aug. 8, 2016), https://securelist.com/analysis/publications/75533/faq-the-projectsauron-apt/ ("ProjectSauron comprises a top-of-the-top modular cyber-espionage platform in terms of technical sophistication . . . The actor behind ProjectSauron has a high interest in communication encryption software widely used by targeted governmental organizations"). These reports may or may not be accurate in their details, but they show that private-sector providers of software security products at least claim to detect efforts to hack governmental networks.

D. Freedom of Choice

A fourth area of divergence, cutting across the other three, is the increased freedom of choice in the use of technology affecting privacy and security, and hence divergence among users in the protection of those two values. As discussed above, digital network technology has, for almost everyone, significantly increased the amount of private information that is created and that may be exposed. But it has also created ways for informed and motivated individuals to significantly reduce that exposure. It's impossible to live off the grid entirely, but it is possible to encrypt sensitive files, to communicate electronically using only encrypted messaging platforms, to choose an extra-long passcode for an iPhone, to use disposable cell phones, to use two-factor authentication for sensitive accounts, to use https as a default, to disable cookies and install ad-blockers and other privacy enhancements in an Internet browser, to avoid Google products and similar "free" offerings that monetize PII, to use TOR, a VPN service, or a proxy server to mask IP addresses and location, and so on.[88] This proliferation of options allows for the worst of both worlds, in which some criminals and terrorists have the incentive to take steps necessary to (partly or wholly) protect themselves from lawful government surveillance (as ISIL recommends to its adherents), while the masses casually remain vulnerable to cyber thefts, attacks, and improper surveillance (whether or not under color of law).[89] Fundamentally, digital divergence shows, we face a world in which the opportunities for improper clandestine communication, theft, influence, and destruction are all proliferating, and the practical ability of individuals, businesses, and governments to defend against those predations, and control their own private data, are diminishing.

IV. Legal Effects of Digital Divergence

This part discusses the effects on constitutional and statutory law that are likely to result in the next few years from digital network technology. The task is difficult because, as explained in Part III, the effects are divergent, creating pressure in both directions. With multiple options for change in each direction, moreover, any one change may reduce pressure that would otherwise support another. Predictions are also hazardous because exogenous variables, like another Snowden leak, the results of an election, and/or a major terrorist attack on the United States, could exert sudden and overwhelming pressure in one direction or another. Subject to those caveats, however, this part of the paper describes how the divergent effects of digital network technology may tend to affect statutory and constitutional law.

A. Legal Change Favoring Privacy

On the side of privacy, Professor Ohm has imagined several changes to Fourth Amendment and statutory law that could follow from an extension of *Riley* and *Jones*,[90] and others have expressed similar ideas.[91] The key elements are as follows:

---

[88] *See, e.g.*, Electronic Frontier Foundation, *Surveillance Self-Defense: Tips, Tools and How-tos for Safer Online Communications*, https://ssd.eff.org.

[89] Of course, some criminals are stupid—they take no special steps to conceal their activities, and they get caught. And some ordinary persons take extraordinary steps to protect their privacy.

[90] *Life of Riley*, *supra* note 12.

• A warrant requirement for any collection of information revealing a person's location for any period of time, including "a single 'ping' on a cell tower," because people "enjoy a reasonable expectation of privacy in their location and movement," including in public places.[92]

---

[91] *See, e.g.*, *supra* note 7.

[92] *Life of Riley*, *supra* note 12, at 135-136, 140. In light of the focus on location information, it is worth reviewing the current state of technology and the law in some detail. In general, digital information concerning a person's location comes in two main types. First, cell site location information (CSLI), which is generated when a cell phone periodically registers with (pings) a base station antenna, or cell site, that is typically mounted on a tower, or when the phone pings a government device that simulates a cell site. The CSLI is not the location of the cell phone *per se*, but rather of the location of the tower(s) and cell site(s) to which the phone connected, which allows inferential plotting of the phone's location over time. In general, the precision of CSLI depends on the local density of towers and antennas (which is generally increasing at least in urban areas). Second, there is more precise information about location that is generated when a cell phone (or other device) connects to the Global Positioning System (GPS) of satellites that orbit the earth, or using multilateration (triangulation via multiple points) and other techniques that rely on the provider's network (for convenience, both true GPS and network techniques of determining precise location are referred to here as GPS). *See generally* Wikipedia, *Mobile Phone Tracking*, https://en.wikipedia.org/wiki/Mobile_phone_tracking. The FCC has mandated that carriers be able to determine location precisely enough to support emergency assistance through its E911 initiative. *See generally Enhanced 9-1-1*, WIKIPEDIA, https://en.wikipedia.org/wiki/Enhanced_9-1-1.

The law in this area is not entirely settled, but in general, CSLI and GPS data are available under different standards depending on whether the data obtained are historical or prospective, and whether they are obtained from a communications provider that generated them in the ordinary course of business or from a special device used by the government (such as a cell site simulator or GPS tracking device). Historical CSLI is generally available under 18 U.S.C. § 2703(d) based on a judicial finding of specific and articulable facts that the CSLI is relevant to a criminal investigation, although some courts have required a warrant based on a showing of probable cause. *Compare, e.g.*, *United States v. Graham*, 824 F.3d 421 (4th Cir. 2016) (en banc), *with*, *In re Application for Telephone Information Needed for a Criminal Investigation*, 119 F. Supp.3d 1011 (N.D. Cal. 2015). As a practical matter, at least, historical CSLI is not available by subpoena or National Security Letter (NSL). *See, e.g.*, *Verizon Transparency Report for the First Half of 2016*, http://www.verizon.com/about/portal/transparency-report/us-report/; *AT&T Transparency Report for the First Half of 2016, Location Demands*, http://about.att.com/content/csr/home/frequently-requested-info/governance/transparencyreport/location-demands.html.The same is likely true of a tangible-things order under FISA, because such an order "may only require the production of a tangible thing if such thing can be obtained with a subpoena duces tecum issued by a court of the United States in aid of a grand jury investigation or with any other order issued by a court of the United States directing the production of records or tangible things." 50 U.S.C. § 1861(c)(2)(D). The law governing access to historical GPS information is not entirely settled, but would likely be influenced by the Supreme Court's decision in *Jones* governing prospective GPS information, discussed below.

As for prospective CSLI, although it likely qualifies as "signaling" information within the definition of a pen register, 18 U.S.C. § 3127, which requires only a certification that the information sought is relevant to a criminal investigation, 18 U.S.C. § 3122, it is not available via criminal pen register based on a specific prohibition enacted in 1994 as part of CALEA, 47 U.S.C. § 1002(a)(2), and this prohibition may also extend to FISA pen registers, 50 U.S.C. 1841, which are understood by the FISA Court of Review to incorporate even some non-definitional elements of the criminal pen-register statutory regime. *See, e.g.*, In re: Certified Question of Law, No. FISCR 16-01 at 17 n.7 (Apr. 14, 2016), https://www.dni.gov/files/icotr/FISCR%20Opinion%2016-01.pdf. In criminal cases, some courts have permitted acquisition of prospective CSLI using "hybrid" (combined) applications for pen registers and Section 2703(d) orders, while others have required search warrants. *See, e.g.*, In re Application, 632 F. Supp. 2d 202, 211 (EDNY 2008); United States v. Espudo, 954 F.Supp.2d 1029 (S.D. Cal. 2013). Prospective CSLI also may not be available under the Wiretap Act because it is not "contents" as defined by 18 U.S.C. 2510(8), *but see* United States v. Beckford, 2012 WL 1980367 (E.D.N.Y. 2012), although a Wiretap Act

• A warrant requirement for any search of stored digital information, because *Riley* effectively "extend[ed] the home" to include effects, and "a police search of an individual's digital information requires at least as much protection as the search of the individual's bedroom," whether that information is on the individual's own hard drive or stored by a third party in the cloud, which is properly viewed as part of the "'virtual curtilage'" of the home.[93]

• Rejection of third-party doctrine beyond the facts of *Smith* and *Miller*, such that (for example) collection of information generated by a fitness tracker device and conveyed voluntarily to a third party remains constitutionally protected, as does all email.[94]

---

interception order requires probable cause and is harder to get than an ordinary search warrant, so the issue is largely one of form, not substance. Prospective CSLI is likely available under a Title I FISA order because FISA defines "contents" more broadly, 50 U.S.C. § 1801(n). In 2015, the Department of Justice adopted a policy generally requiring a warrant based on probable cause (as well as the requirements of a pen register) for the use of a cell-site simulator to obtain CSLI in the United States. Department of Justice Policy Guidance: Use of Cell-Site Simulator Technology at 1 n.1 (2015), https://www.justice.gov/opa/file/767321/download ("When acting pursuant to the Foreign Intelligence Surveillance Act, Department of Justice components will make a probable-cause based showing and appropriate disclosures to the court in a manner that is consistent with the guidance set forth in this policy.") In other words, the government must obtain a Title I or II FISA order, which requires a showing of probable cause.

It is reasonably clear after the Supreme Court's decision in *Jones* that, in the view of five Justices, extended prospective GPS monitoring, whether or not accomplished through the physical attachment or use of a special device, requires a warrant or other judicial order based on probable cause (including a FISA order). *But cf.* United States v. Skinner, 690 F.3d 772 (6th Cir. 2012) (distinguishing *Jones* where GPS tracking was accomplished using the defendant's cell phone and surveillance was only for three days, not 28 days as in *Jones*).

[93] *Life of Riley*, *supra* note 12, at 136-137. The Supreme Court has explained the "curtilage" of a home as follows:

> The curtilage concept originated at common law to extend to the area immediately surrounding a dwelling house the same protection under the law of burglary as was afforded the house itself. The concept plays a part, however, in interpreting the reach of the Fourth Amendment. *Hester v. United States* held that the Fourth Amendment's protection accorded "persons, houses, papers, and effects" did not extend to the open fields . . . We reaffirmed the holding of *Hester* in *Oliver v. United States*. There, we recognized that the Fourth Amendment protects the curtilage of a house and that the extent of the curtilage is determined by factors that bear upon whether an individual reasonably may expect that the area in question should be treated as the home itself. We identified the central component of this inquiry as whether the area harbors the "intimate activity associated with the 'sanctity of a man's home and the privacies of life.'"

United States v. Dunn, 480 U.S. 294, 300 (1987) (citations omitted). The Court has not extended the concept to the digital realm. For a discussion of the concept of a "personal curtilage," see Andrew Guthrie Ferguson, *Personal Curtilage: Fourth Amendment Security in Public*, 55 Wm. & Mary L. Rev. 1283 (2014).

[94] *Life of Riley*, *supra* note 12, at 137-138, 140-141. In United States v. Miller, 425 U.S. 435 (1976), the Court rejected the defendant's claim that he "has a Fourth Amendment interest in the records kept by the banks because they are merely copies of personal records that were made available to the banks for a limited purpose and in which he has a reasonable expectation of privacy." *Id*. at 441. The Court explained: "Even if we direct our attention to the original checks and deposit slips, rather than to the microfilm copies actually viewed and obtained by means of the subpoena, we perceive no legitimate 'expectation of privacy' in their contents. The checks are not confidential communications but negotiable instruments to be used in commercial transactions. All of the documents obtained, including financial statements and deposit slips, contain only information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business." *Id*. at 442. In *Smith v. Maryland*, 442 U.S. 735

• Rejection of the idea that minimization and other limits on the retention, use, and dissemination of data can save the constitutionality of an otherwise overbroad acquisition of data, whether for purposes of ordinary law enforcement or national security.[95]

• A conclusion that FISA's tangible things provision, and perhaps also a grand jury subpoena and pen register, cannot be used to obtain URLs and other "web browsing data."[96]

(1979), the Court relied on *Miller* to uphold the warrantless installation and use of a pen register, which only records the numbers dialed in a telephone call.

Although *Miller* was rooted in the informant cases—in which a speaker was deemed to have assumed the risk that his interlocutor would tell the police what he said—there would be room, in a future case, for the Supreme Court to limit third-party doctrine in various ways, perhaps excluding common carriers (rather than individuals) or excluding financial transactions (rather than communications). The Sixth Circuit has held that "a subscriber enjoys a reasonable expectation of privacy in the contents of emails that are stored with, or sent or received through, a commercial ISP," that the "government may not compel a commercial ISP to turn over the contents of a subscriber's emails without first obtaining a warrant based on probable cause," and that "to the extent that [federal statutory law] purports to permit the government to obtain such emails warrantlessly, [it] is unconstitutional." United States v. Warshak, 631 F.3d 266, 288 (6th Cir. 2010) (citations and internal quotations omitted). The same approach is likely to apply to other forms of electronic communications. *See, e.g.*, United States v. Bode, 2013 WL 4501303 (D. Md. Aug. 21, 2013) (citing cases involving email, faxes, text messages, and Facebook messages).

[95] *Life of Riley*, *supra* note 12, at 138-139. One of the examples cited involves the Foreign Intelligence Surveillance Court, which has held that minimization procedures can affect the constitutionality of an otherwise-overly broad acquisition, as discussed in NSIP § 17:5 (supplement). The other involves a criminal seizure and contemporaneous search of a computer hard drive pursuant to warrant, and then a second search years later in a different investigation pursuant to a different search (not seizure) warrant. In August 2016, the government released an opinion of the Foreign Intelligence Surveillance Court of Review permitting acquisition with a FISA pen-register of post cut-through digits, some of which may be "contents," in part because of strict protocols limiting any subsequent use of the contents. *See* In re: Certified Question of Law, No. FISCR 16-01 at 17 n.7 (Apr. 14, 2016), https://www.dni.gov/files/icotr/FISCR%20Opinion%2016-01.pdf. As discussed in *Trends and Predictions*, *supra* note 37, there is likely to be renewed debate about government's authority to query acquired data without considering the query as the effective equivalent of a new search. Thus, while the privacy narrative's prescription may reject the idea that post-acquisition protocols can justify broader acquisition, it also may include the idea of requiring such protocols for digital data.

[96] *Life of Riley*, *supra* note 12, at 139. Section 215 of the USA Patriot Act amended FISA, 50 U.S.C. § 1861, to permit orders from the FISC compelling the production of tangible things. *See* NSIP Chapter 19. The FISA Court has authorized acquisition of post cut-through digits using a pen register, but the FISA Court of Review has cautioned that this approach might raise different issues in the context of Internet pen registers. *See* In re: Certified Question of Law, No. FISCR 16-01 at 17 n.7 (Apr. 14, 2016), https://www.dni.gov/files/icotr/FISCR%20Opinion%2016-01.pdf. It is not clear whether and how certain web-browsing data, such as requests using an online search engine, are protected by the Constitution or statute. *See Miller* and *Smith*, *supra* note 94, discussion of third-party doctrine. However, the Center for Democracy and Technology has published on its website an unclassified document purporting to be the Department of Justice's answers to certain frequently asked questions about the use of certain surveillance authorities. *See* https://cdt.org/insight/responding-to-the-dojs-faq-on-the-use-of-nsls-to-compel-communications-providers-to-produce-ectrs/. According to that document, DOJ has accepted the courts' judgment that only the fully qualified domain name—the information before the first slash in a URL—is treated as non-contents, and thus available under provisions such as national security letters that do not require a showing of probable cause.

• A rejection of warrantless border searches of hard drives or other digital data.[97]

• A warrant requirement before the government can engage in self-help to decrypt digital data, and a requirement for detailed search protocols in any warrant to search digital data, even if that approach hinders law enforcement and reduces security.[98]

Some of these changes would significantly change current law; others would reinforce or extend existing trends. Together, they are a reasonably good description of changes in law that respond to digital network technology with the aim of increasing protection of privacy.

A supplement to Professor Ohm's list might include greater regulation of drones and aerial surveillance,[99] tighter restrictions on government's use of publicly available information,[100] and an overhaul of the Electronic Communications Privacy Act (ECPA), which is badly out of date nearly 30 years after its enactment.[101] ECPA regulates providers of "electronic communications service" (ECS)[102] and "remote computing service" (RCS),[103] terms defined in ways that do not correspond perfectly to the current menagerie of digital network providers and

[97] *Life of Riley*, *supra* note 12, at 139. As the Supreme Court has explained, "[s]ince the founding of our Republic, Congress has granted the Executive plenary authority to conduct routine searches and seizures at the border, without probable cause or a warrant, in order to regulate the collection of duties and to prevent the introduction of contraband into this country." United States v. Montoya de Hernandez, 473 U.S. 531, 537 (1985)..

[98] *Life of Riley*, *supra* note 12, at 140-141. For a discussion of such protocols, *see* United States v. Comprehensive Drug Testing, Inc., 621 F. 3d 1162 (2010).

[99] *See, e.g.*, Daniel Wilson, *FAA Sued Over Lack of Privacy Controls in Final Drone Rule*, Law360 (Aug. 23, 2016), http://www.law360.com/articles/831782/faa-sued-over-lack-of-privacy-controls-in-final-drone-rule; Michael Sheehan, *U.S. Citizens' Fourth Amendment Rights & Unmanned Aerial Vehicles: An Appeal for Bright-Line Legislative Action*, 32 TEMP. J. SCI. TECH. & ENVTL. L. 255 (2013).

[100] In August 2016, the government released an updated version of DOD Manual 5240.01, the basic procedures, subordinate to Executive Order 12333, for DOD agencies with respect to collection of U.S. person information. *See* http://www.dtic.mil/whs/directives/corres/pdf/524001m.pdf. As explained in an accompanying Fact Sheet, https://www.documentcloud.org/documents/3010006-DOD-Guidelines-Fact-Sheet-08-08-2016-FINAL-1120.html, one of the "[m]ajor changes" to the DOD rules is an updated definition of "publicly available information." Fact Sheet at 1. The changes are designed to provide "a more detailed characterization of what 'publicly available' means, recognizing the policy issues raised by the Internet and new technology." Fact Sheet at 2. The topic is worthy of extended discussion, but for present purposes it is enough to note that among the most challenging issues with respect to publicly available information are the treatment of bulk collection, the use of queries and other analytical methods on unevaluated information, the role of undisclosed participation in groups by government agents, the elicitation of publicly available information by government agents, and the rules governing undisclosed participation and elicitation in social media and on the Internet. In all of these areas, the rules could become more restrictive.

[101] Electronic Communications Privacy Act (ECPA), which includes the SCA, became law on October 21, 1986, as Pub. L. No. 99-508, 100 Stat. 1848. It has been amended since then, but not comprehensively.

[102] 18 U.S.C. § 2710(15). An ECS includes an ISP and providers of email service.

[103] 18 U.S.C. § 2711(2). An RCS includes a cloud storage provider.

the services they offer.[104] Also, the statute provides less protection for email that is older than 180 days,[105] and perhaps for email that has been opened[106]—distinctions that may have made sense in 1986, but seem arbitrary and arguably unconstitutional today.[107]

B. Legal Change Favoring Security

On the side of security, the prescription is less well developed, and perhaps more complex. Possible changes include abandonment of location-based paradigms for regulation of surveillance; revisions of ECPA and perhaps the Foreign Intelligence Surveillance Act (FISA)[108] as needed to permit acquisition of data stored abroad (or clarify that such acquisition is permitted); more international agreements, supplementing existing Mutual Legal Assistance Treaties, allowing governments direct access to data held by providers outside their borders (e.g., allowing the UK government to obtain data directly from Microsoft); a more robust requirement for communications providers to assist government with decryption; greater governmental access to metadata; and either much more voluntary cooperation between government and the private sector or more regulation of digital networks, including the Internet.

The first of the threats to security cited in Part II, the growing anonymity and indeterminacy of the location of people using digital networks, is not new. It received significant attention more than eight years ago, when Congress enacted the FISA Amendments Act (FAA) of 2008, but it has receded since then. Prior to the amendments, FISA's regulatory reach depended in large part on the location of both the sender and recipients of a communication (e.g., a live telephone call or email message). As I have explained elsewhere,[109] the FAA updated FISA in light of "web-based e-mail and other developments [which] made it more difficult to determine the location of parties to an intercepted communication."[110] 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 (or any other factor).[111]

---

[104] *See, e.g.*, Kurt Young, Jr., *Privacy Law in the Digital Age: Establishing Privacy Rights in Search Engine Logs*, 14 Conn. Pub. Int. L.J. 157 (2015).

[105] *See* 18 U.S.C. § 2703(a)-(b).

[106] *See* 18 U.S.C. § 2510(17); Cobra Pipeline Ltd. v. Gas Natural, Inc., 132 F. Supp.3d 945, 949-950 (N.D. Oh. 2015) (citing conflicting cases).

[107] *See* United States v. Warshak, 631 F.3d 266, 288 (6th Cir. 2010).

[108] 50 U.S.C. § 1801 *et seq*.

[109] *See, e.g., Trends and Predictions, supra* note 37.

[110] *Id*. at 2.

[111] *Id*.

However, the FAA still requires the government to form a "reasonable belief" as to the target's location, and this can be challenging. There are many ways to spoof physical location on digital networks, and "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."[112] Given this requirement to resolve conflicting information, "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."[113] To be sure, 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. But [if 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."[114] One of the possible effects of digital network technology, therefore, may be the eventual demise of legal paradigms based on location of surveillance targets. At present, there is no replacement paradigm.[115]

The second factor, concerning the location of data (rather than people), is best illustrated by the Second Circuit's July 2016 *Microsoft* decision, and by recent challenges in dealing with cross-border data requests. In the *Microsoft* case, the Second Circuit held that the U.S. Stored Communications Act (SCA)[116] does not allow the government to compel the production of email messages stored outside the United States. Relying on the presumption against "extraterritorial" application of U.S. laws, and reinforced by the SCA's use of the inherently territorial word "warrant" to describe the instrument of compelled production it authorizes, the court held that applying the SCA to data stored on a server in Dublin, Ireland, was indeed extraterritorial, and beyond the scope of the warrant. The court reached that conclusion because, it found, the "focus" of the SCA was protecting privacy, and "it is our view that the invasion of the customer's privacy takes place under the SCA where the customer's protected content is accessed—here,

---

[112] *Id.* at 24.

[113] *Id*. In its 2015 transparency report, ODNI made clear that while it refers to nearly 100,000 "targets" under the FAA, it may be more accurate to think about "selectors" (e.g., email addresses, telephone numbers, or other communications facilities), because "foreign intelligence targets often communicate using several different email accounts. Each email account is a different selector, so unless the Intelligence Community has information that multiple email accounts are used by the same target, each of those accounts, i.e., selectors, would be counted separately in these figures" as a discrete target. This "helps ensure that the Intelligence Community does not inadvertently understate the number of discrete persons targeted pursuant to Section 702," but almost surely results in an overstatement, perhaps a significant overstatement. 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.

[114] *Id*. (italics in original).

[115] Citizenship as a regulatory criterion is also under pressure. In substantial part, U.S. government protocols presume the citizenship of an unknown target based on the target's location. It is therefore possible that we will see legal changes extending PPD-28, which erodes privacy distinctions between U.S. and non-U.S. persons, as discussed in *NSIP* Chapter 19.

[116] 18 U.S.C. §§ 2701 *et seq*.

where it is seized by Microsoft, acting as an agent of the government" in Ireland, not where the content is delivered to or first reviewed by government agents, in the United States. "Because the content subject to the Warrant is located in, and would be seized from, the Dublin datacenter, the conduct that falls within the focus of the SCA would occur outside the United States, regardless of the customer's location and regardless of Microsoft's home in the United States."[117]

Judge Lynch concurred in the *Microsoft* case, primarily to "emphasize the need for congressional action to revise a badly outdated statute."[118] He explained that under "Microsoft's and the Court's interpretation of the SCA, the privacy of Microsoft's customers' emails is dependent not on the traditional constitutional safeguard of private communications—judicial oversight of the government's conduct of criminal investigations—but rather on the business decisions of a private corporation."[119] Put differently, *Microsoft may now enjoy unilateral authority to block collection of any email under the primary statute used by federal law enforcement to acquire it*. Alternatively, as Judge Lynch explained, "The contract between Microsoft and its customers does not limit the company's freedom to store its customers' emails wherever it chooses, and if Microsoft chooses, for whatever reasons of profit or cost control, to repatriate the emails at issue here to a server in United States, there will be no obstacle to the

[117] 2016 WL 3770056, at *15-*17. This conclusion was by no means inevitable, and on October 13, 2016, the government filed a petition for rehearing en banc, which remains pending as of this writing. No. 14-2985 (Oct. 13, 2016), https://dlbjbjzgnk95t.cloudfront.net/0851000/851585/microsoft%20rehearing%20.pdf. For example, in the context of the federal Wiretap Act, which generally prohibits the interception of live wire or electronic communications, courts have held that the prohibition does not apply extraterritorially, with extraterritoriality determined according to where the "interception" occurs, because interception is the focus of the statute. But the courts have also held that "interception occurs where the tapped phone is located *and* where law enforcement officers first overhear the call," such that the statute applies if *either* of those events occur in the United States. United States v. Luong, 471 F.3d 1107, 1109 (9th Cir. 2006) (citing cases) (italics in original). For example, in United States v. Rodrigue*z*, 968 F.2d 130, 136 (2d Cir. 1992), the court explained:

> It seems clear that when the contents of a wire communication are captured or redirected in any way, an interception occurs at that time. Such an interception plainly occurs at or near the situs of the telephone itself, for the contents of the conversation, whether bilateral as is usually the case, or multilateral as is the case with a conference call, are transmitted in one additional direction. Redirection presupposes interception. Accordingly, a federal court sitting in the jurisdiction in which the to-be-tapped telephone is located would have the authority, under [18 U.S.C.] § 2518(3), to authorize a wiretap. Nonetheless, since the definition of interception includes the 'aural' acquisition of the contents of the communication, the interception must also be considered to occur at the place where the redirected contents are first heard.

See also Huff v. Spaw, 794 F.3d 543, 547 (6th Cir. 2015) (concluding that prohibition on interception applies to an accidentally-made international cell phone call that allowed a person in the United States surreptitiously to monitor an oral discussion occurring between two persons located in Italy, one of whom had the phone in a back pocket). On this approach, the *Microsoft* court could have concluded that the SCA is territorial (and a proper warrant), rather than extraterritorial, where the government first reads the email in the United States, particularly because Microsoft could have acted in the U.S. to repatriate the email from Ireland. *See* 2016 WL 3770056, at *3 ("Microsoft acknowledges that, by using a database management program that can be accessed at some of its offices in the United States, it can 'collect' account data that is stored on any of its servers globally and bring that data into the United States.").

[118] 2016 WL 3770056, at *19.

[119] *Id*. at *20.

government's obtaining them," because a neutral and detached magistrate found probable cause that they contained evidence of a crime.[120] Given those possibilities, the need for legislation was evident, at least to Judge Lynch:

> Reasonable people might conclude that extremely stringent safeguards ought to apply to government investigators' acquisition of the contents of private email communications, and that the provisions of the SCA, as applied domestically, should be enhanced to provide even greater privacy, at an even higher cost to criminal investigations. Other reasonable people might conclude that, at least in some cases, investigators should have freer access to stored communications. It is the traditional task of Congress, in enacting legislation, and of the courts, in interpreting the Fourth Amendment, to strike a balance between privacy interests and law enforcement needs. *But neither privacy interests nor the needs of law enforcement vary depending on whether a private company chooses to store records here or abroad – particularly when the "records" are electronic zeros and ones that can be moved around the world in seconds, and will be so moved whenever it suits the convenience or commercial purposes of the company*. The issue facing the Court, then, is not actually about the need to enhance privacy protections for information that Americans choose to store in the "cloud."[121]

As I have explained elsewhere, there is a similar problem with the FISA statute: "[W]hen e-mail is stored abroad, neither traditional FISA nor the FAA can be used to compel provider assistance [in producing the e-mail] if the target is either a U.S. 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."[122] Although the government has said it will seek legislation to remedy the *Microsoft* decision,[123] it has not done so yet, and it has not even addressed the question of amending FISA, at least in public.[124]

---

[120] *Id*. at *20. If Microsoft were to move data abroad *after* receiving a warrant for the data (or otherwise becoming aware that the government was seeking the data), it might raise several issues. But there does not appear to be a U.S. legal prohibition on Microsoft moving data abroad in general, and European data privacy directives would not restrict moving data from the United States to Europe.

[121] *Id*. at *21 (italics added).

[122] *Trends and Predictions*, *supra* note 37, at 21.

[123] On July 15, 2016, the government submitted a letter to Congress stating that it intends "to promptly submit legislation to Congress to address the significant public safety implications of the *Microsoft* decision." Letter from Peter J. Kadzik to Jospeh R. Biden at 3, https://www.documentcloud.org/documents/2994379-2016-7-15-US-UK-Biden-With-Enclosures.html#document/p1. As of this writing, it has not done so. As noted above, on October 13, 2016, it filed a petition for rehearing en banc. This filing may reflect the administration's inability to settle on a legislative proposal, and/or it may reflect a preference for orderly resolution of issues, exhausting judicial review of existing laws before seeking legislative correction.

[124] The relative silence on FISA could be attributable to several factors. First, perhaps my analysis is simply incorrect, and there is indeed no problem. Second, perhaps providers have not widely invoked the analysis to resist FISA warrants—a reticence that could stem from a desire to avoid fighting with the government in the context of a FISA warrant (which involves national security) as opposed to an SCA warrant (which involves ordinary criminals, like drug dealers), or from providers not knowing, or wanting to determine, the location of their data in each case.

A related problem arising from the mobility of data concerns cross-border data requests. These involve situations in which, as I have described elsewhere, "one government's laws compel the production of information while another government's laws simultaneously forbid that same production. For example, the UK has been terribly frustrated by its inability to compel American communications providers, like Microsoft, to provide email that resides on servers in the United States but is from the account of a suspected terrorist located in Britain and planning attacks there. UK law can be used to compel such production, but current U.S. law forbids it."[125] For another example, Microsoft has been fined millions of dollars, and its employees threatened with criminal prosecution, for following a U.S. law that makes it a crime to obey a Brazilian court order demanding information about a suspected criminal in Brazil.[126]

Here the U.S. government has proposed legislation to address the problem, in the form of a set of proposed legislative amendments that would allow for executive agreements between the U.S. and select foreign governments, allowing each government direct access to data that would otherwise be unavailable due to the other government's law. But the process of generating the draft legislation, even within the Executive Branch, took more than a year, and debate over the proposal in Congress has not yet begun in earnest. Meanwhile, the U.S. and Britain are advised to use their Mutual Legal Assistance Treaty, under which each request for data takes several months to fulfill.

A third challenge involves encryption. As noted above, encryption has received a good deal of attention, and has spawned a massive recent literature.[127] The major challenge, which remains unresolved, is how to permit lawful access to data while protecting against unlawful access. The fundamental claim of many industry and privacy professionals is that encryption systems cannot be designed to permit the former without unduly risking the latter. The fundamental belief of many security and law enforcement professionals is that industry and privacy advocates have not seriously tried to find a viable solution. The most promising approach identified so far involves some version of relying on encryption using multiple keys, at least one of which would be held by providers (who already maintain keys used to validate

---

See, e.g., Devlin Barrett & Jay Greene, *U.S. to Allow Foreigners to Serve Warrants on U.S. Firms*, WALL ST. J. (July 15, 2016), http://www.wsj.com/article_email/obama-administration-negotiating-international-data-sharing-agreements-1468619305-lMyQjAxMTA2NjE1NTMxNTUzWj. Third, any change to address the problem may risk expanding FISA's scope in such a way that other intelligence activity would become regulated by the statute, rather than by EO 12333 and its subordinate procedures. Fourth and finally, it may be that the law enforcement and national security professionals within government who understand the problem have concluded that any effort to seek enhanced FISA authority is doomed to failure or backfire, either within the Executive Branch itself or through engagement with Congress.

[125] David Kris, *U.S. Government Presents Draft Legislation for Cross-Border Data Requests,* LAWFARE (July 16, 2016) [hereinafter *Cross-Border Legislative Proposal*], https://www.lawfareblog.com/us-government-presents-draft-legislation-cross-border-data-requests; *see Cross-Border Data Requests*, *supra* note 84.

[126] *Cross-Border Legislative Proposal*, *supra* note 125.

[127] *See, e.g.*, https://www.lawfareblog.com/search/node/encryption.

software updates to operating systems or applications).[128] But even if that approach proves viable in general, much work remains to be done on the details.

In the meantime, one school of thought is best described as "Don't Panic," mainly on the grounds that providers' desire to scan the contents of email and other electronic messages for purposes of selling targeted advertising will limit the spread of encryption, and that metadata will remain available because it cannot be encrypted without preventing the proper routing and addressing of messages across packet-switched networks.[129] The government, however, is not as sanguine, because it believes that encrypted channels will likely attract the most sophisticated and dangerous adversaries, and that metadata, while valuable, is no substitute for contents.[130]

Encryption is likely to create legal change under the rubric of "compelled assistance" from providers, as I have discussed elsewhere.[131] In the meantime, if and to the extent that government continues to come forward with examples of how encryption hinders investigations, the courts and Congress may feel increased pressure to ease limits on access to metadata. In August 2016, for example, the government released an opinion by the Foreign Intelligence Surveillance Court of Review affirming the practice of allowing the government to acquire all post cut-through digits using a telephone pen register, even though some of those digits may

---

[128] One thoughtful commentator on this issue is Matt Tait, formerly employed by GCHQ, the British analogue to NSA. In a recent blog post, Tait claimed that Apple may have inadvertently disclosed an approach that would allow decryption pursuant to lawful court order without unduly increasing the attack surface or risk of unauthorized decryption. Matt Tait, *Apple at BlackHat: Reopening the "Going Dark" Debate*, LAWFARE (Aug. 12, 2016), https://www.lawfareblog.com/apple-blackhat-reopening-going-dark-debate; *see also* Matt Tait, *An Approach to James Comey's Technical Challenge*, Lawfare (Apr. 27, 2016), https://www.lawfareblog.com/approach-james-comeys-technical-challenge.

[129] *See, e.g.*, *Don't Panic: Making Progress in the "Going Dark" Debate*, Berkman Center, Harvard University (Feb. 1, 2016), https://cyber.law.harvard.edu/pubrelease/dont-panic/; *see also* The Chertoff Group, *The Ground Truth About Encryption* (2016), https://chertoffgroup.com/cms-assets/documents/238024-282765.groundtruth.pdf. *Cf., e.g.*, Kat Sieniuc, *Google Can't Escape Gmail Privacy Suit, Judge Says* (Aug. 15, 2016) ("A California federal judge on Friday denied Google's bid to toss a proposed class action accusing the company of scanning emails for advertisers, ruling the practice is not considered part of the company's day-to-day operations under federal wiretapping laws."), http://www.law360.com/california/articles/828337?utm_source=shared-articles&utm_medium=email&utm_campaign=shared-articles.

[130] *See, e.g.*, Letter from Deirdre M. Walsh, ODNI, to Senator Ron Wyden (May 6, 2016), https://www.wyden.senate.gov/download/?id=3F716160-095E-420E-93F3-849453EB61B2&download=1. As an example of the risks of encryption, government officials describe a scenario in which a known terrorist meets a potential recruit online, they engage in a discussion that is protected by the First Amendment and does not supply probable cause, and then as the discussion progresses, the recruiter suggests moving to an encrypted channel like WhatsApp. The government knows that the discussion is continuing, but not what is being said and whether the potential recruit has agreed to take violent action. *See, e.g.*, James Comey, *Counterterrorism, Counterintelligence, and the Challenges of Going Dark* (July 8, 2015), https://www.fbi.gov/news/testimony/counterterrorism-counterintelligence-and-the-challenges-of-going-dark; James Comey, *Expectations of Privacy: Balancing Liberty, Security, and Public Safety* (Apr. 6, 2016), https://www.fbi.gov/news/speeches/expectations-of-privacy-balancing-liberty-security-and-public-safety ("It seems like a lifetime ago, WhatsApp announced that encryption moved on all of their services yesterday. A billion people now communicating in ways that can't be intercepted even with a judge's order.")

[131] *See Trends and Predictions*, *supra* note 37, at 16-21.

constitute the "contents" of a communication that is not legally available using a pen register.[132] Although a pen register is defined as a device or process that acquires certain types of metadata that "shall not include the contents of any communication,"[133] a related provision, not expressly incorporated into FISA, directs government agencies that use a pen register to "use technology reasonably available to it that restricts the recording or decoding of electronic or other impulses . . . so as not to include the contents" of a communication.[134] The court found that "[u]nder presently available technology, there is no way for a pen register to distinguish between dialing information and content information contained in post-cut-through digits so that it can be directed to intercept only the former and not the latter."[135] Thus, the court had to decide whether to forbid all acquisition of post cut-through digits, which would allow any sophisticated adversary to defeat a pen register by using a calling card, or to permit the acquisition subject to strict limits on the use of any post cut-through digits determined later to be contents. The court chose the latter approach, rejecting the contrary conclusions of a few district courts in ordinary criminal cases.[136]

One related effect, far-fetched today but perhaps possible in the future, would be to shift standards governing expectations of privacy for purposes of the Fourth Amendment. As Justice Alito recognized in *Jones*, "reasonable" expectations of privacy are culturally contingent,[137] and if privacy-enhancing options become as widely understood and employed as basic smartphone technology is today, it is possible to imagine a different outcome in *Riley*, in which the Court concludes that failing to encrypt and auto-lock your smartphone is analogous to exhibitionism, a voluntary surrender of any reasonable expectation of privacy.[138] Private-sector business models

---

[132] *In re: Certified Question of Law*, No. FISCR 16-01 at 17 n.7 (Apr. 14, 2016) [hereinafter FISCR Cut-Through Opinion], https://www.dni.gov/files/icotr/FISCR%20Opinion%2016-01.pdf. The reference to "post cut-through" digits is to numbers dialed by a caller after a call has been connected, or cut through. One example of post cut-through digits that would be "contents" is a password entered on a telephone to obtain a bank account balance; an example of post cut-through digits that (most observers) would consider not to be "contents" is the telephone number dialed after connecting to an 800 number using a calling card. *Cf.* Orin Kerr, *Relative vs. Absolute Approaches to the Content/Metadata Line*, LAWFARE (Aug. 25, 2016), https://lawfareblog.com/relative-vs-absolute-approaches-contentmetadata-line.

[133] 18 U.S.C. § 3127(3).

[134] 18 U.S.C. § 3121(c).

[135] FISCR Cut-Through Opinion, *supra* note 132, at 7.

[136] *Id.* at 11-12.

[137] In his concurring opinion in *Jones*, 132 S. Ct. at 962, Justice Alito explained that the "expectation-of-privacy test . . . rests on the assumption that [the] hypothetical reasonable person has a well-developed and stable set of privacy expectations. But technology can change those expectations. Dramatic technological change may lead to periods in which popular expectations are in flux and may ultimately produce significant changes in popular attitudes. New technology may provide increased convenience or security at the expense of privacy, and many people may find the tradeoff worthwhile. And even if the public does not welcome the diminution of privacy that new technology entails, they may eventually reconcile themselves to this development as inevitable."

[138] The idea would be that leaving data unencrypted is analogous to abandoning it on the side of the road, *cf.* California v. Greenwood, 486 U.S. 35, 40 (1988), or to leaving a door or window open for police officers to peer in, *cf.* United States v. Wright, 991 F.2d 1182, 1186 (4th Cir. 1991).

that rely on monetization of personally identifiable information—to the extent they become widely understood and remain widely tolerated—may themselves erode societal expectations of privacy in ways that effectively reduce Fourth Amendment protections.

The fourth challenge is Fintech. Today, bitcoin and other digital currencies are regulated primarily as property or commodities rather than as money.[139] As a result, they have not yet been subject to the full scope of banking regulations. The U.S. Treasury's FinCEN issued guidance in 2013 regulating exchangers and administrators of digital currencies, and New York enacted a statute in 2015 regulating those involved with digital currencies as a business, including a requirement to file suspicious activity reports. Some of the increasing regulation here is due to the complexity of the banking laws and the novelty of digital currency. But it is easy to see how a terrorist attack that was facilitated or funded by digital currency could give rise to greater regulation, including wider and stricter application of know-your-customer, anti-money laundering, and other requirements.[140]

One more technological challenge for surveillance is the problem of too much data. Until 2013, the government's approach to this challenge was to collect data in bulk even in the United States under FISA, and to adopt relatively strict requirements on retention, use, and dissemination of the data. This approach had been accepted by all three branches of the federal government. The firestorm resulting from the Snowden disclosures, however, changed that. As a result, the new preferred approach is something more like the USA Freedom Act, which forbids bulk collection under FISA's pen-register and tangible things provisions and national security letters (NSLs), leaving data with the communications providers who retain it as they see fit for business reasons, and allowing iterative queries of the data by government to reveal connections and patterns.[141] This approach reduces the amount of data held by the government, but it may be more expensive and more difficult to scale across multiple providers. In any event, it is now pretty clearly the dominant paradigm for collection under FISA and NSLs, and will likely remain in place unless and until it proves inadequate. One possible addition would be explicit requirements for providers to retain data for certain periods of time—an approach not pursued in the USA Freedom Act itself.

Finally, the effects of other challenges that facilitate misconduct—e.g., cyber issues, the Dark Web, ungoverned spaces—could, at their most extreme, lead to significant changes at the network level, if not the individual level, of digital activity. These changes could include greater regulation of the Internet and communications technologies (or greatly increased voluntary cooperation between government and the private sector). They could include automated or blended responses to cyber threats—e.g., an expanded and enhanced version of a cyber defense system like Einstein 3 for the whole U.S. Internet (not merely for the .gov domain), perhaps

---

[139] *See* John L. Douglas, *New Wine into Old Bottles: Fintech Meets the Bank Regulatory World*, 20 N.C. Banking Inst. 17 (Mar. 2016).

[140] *See id*.

[141] For a discussion of bulk collection of metadata, and the USA Freedom Act, *see NSIP* Chapter 19 (2016 supplement). It is important to note that Section 2 of PPD-28 expressly contemplates bulk collection under other authorities, such as Executive Order 12333.

coupled with kinetic aspects.[142] Or it could involve the attempted removal of some critical infrastructure from connection to digital networks. Today, of course, many of these notions are political non-starters.[143] But in the aftermath of a catastrophic attack, understood to have been enabled by one or more of the digital threats discussed above (e.g., encryption), public opinion could shift.[144] To enable certain of the most extreme changes, the shift would need to be dramatic enough that U.S. citizens begin thinking of the Internet as something more like the commercial air traffic system, with screening of persons and goods required for entry, government supervision and safety standards for privately-owned and -operated equipment, and the like.[145]

V. Conclusion

Digital network technology provides many benefits, but has reduced both privacy and security. One of the great challenges in the years ahead will be to find ways to change that trend. This paper attempts to assist that effort by summarizing the ways in which digital network technology threatens privacy; by identifying, developing and synthesizing the ways in which it threatens security; by examining those two narratives jointly within the framework of digital divergence; and by outlining some of the possible effects of this divergence on statutory and constitutional law. Some of those effects are mutually exclusive, and so require hard choices, but others are mutually compatible.

A few weeks before publication of Edward Snowden's first leak, I published a series of blog posts discussing the possibility of a "blue sky" overhaul of U.S. surveillance law.[146] I explained that a "blue-sky overhaul, while easy to imagine, would be extraordinarily difficult to

---

[142] For a description of Einstein 3, *see* Department of Homeland Security, *Privacy Impact Assessment for Einstein 3* (2013), https://www.dhs.gov/sites/default/files/publications/PIA%20NPPD%20E3A%2020130419%20FINAL%20signed.pdf. This is not to suggest that Einstein 3, even if it were extended to the whole U.S. Internet, would be sufficient to satisfy the demands of the strongest form of the security narrative. The point is only that even the *starting point* for this kind of thinking would be considered radical by many observers today. *Cf.* Sam Jones, *Spymasters Plan to Build "Great British Firewall"*, FIN. TIMES (Sept. 13, 2016), http://www.ft.com/cms/s/0/85549652-79d1-11e6-97ae-647294649b28.html#axzz4KI2sOcRJ.

[143] *Cf., e.g.*, David Ignatius, *Let the Geeks Rule Over the Internet*, THE WASH. POST (Aug. 2, 2016), https://www.washingtonpost.com/opinions/let-the-geeks-rule-over-the-internet/2016/08/02/7121eb68-58f6-11e6-9767-f6c947fd0cb8_story.html?utm_term=.ef025a06fbe9; Paul Rosenzweig, *Is Encryption Driving Everyone Crazy?*, LAWFARE (Apr. 14, 2016), https://www.lawfareblog.com/encryption-driving-everyone-crazy.

[144] *Cf., e.g.*, Zeke Turner, *Germans Reconsider Tough Privacy Laws After Terrorist Attacks*, WALL ST. J. (Aug. 19, 2016), http://www.wsj.com/articles/germans-reconsider-tough-privacy-laws-after-terrorist-attacks-1471628581.

[145] Airports enable tremendous domestic and international commerce and interaction, may house shops and other commercial establishments, and serve private-sector airlines. But airports, and most other aspects of the commercial aviation system, are also heavily-regulated critical infrastructure. It seems appropriate here to reiterate that I am not advancing any policy prescription in this paper, either in favor of privacy or security, but rather *describing* ways of thinking about digital network technology from the perspective of privacy and security, and considering the possible legal and related effects that could result from those ways of thinking.

[146] David Kris, *Thoughts on a Blue-Sky Overhaul of Surveillance Law*, LAWFARE (May 18, 2013), https://www.lawfareblog.com/thoughts-blue-sky-overhaul-surveillance-laws-introduction.

execute, fraught with risk, and likely to fail in practice," but that if the pain caused by the existing system were to "escalate sufficiently, or if there is a crisis of some sort, an overhaul may become possible or required despite the risks and costs."[147] Digital network technology has the potential to upset many of our established rules and practices— not in a single, paroxysmal burst of new law created intentionally by elected officials, but through a rapid and radical transformation of the environment underlying the old law fueled by commercial motives. I have tried, in this paper, to help us keep up with that transformation.

[147] *Id.*