UNC SCHOOL OF LAW

NORTH CAROLINA JOURNAL OF LAW & TECHNOLOGY

Volume 14
Issue 2 *U.S. v. Jones: Defining a Search in the 21st Century (Symposium Issue)*

Article 6

3-1-2013

Jonesing for a Privacy Mandate, Getting a Technology Fix - Doctrine to Follow

Stephanie K. Pell

NORTH CAROLINA JOURNAL OF LAW & TECHNOLOGY
VOLUME 14, ISSUE 2: SPRING 2013

*JONES*ING FOR A PRIVACY MANDATE, GETTING A TECHNOLOGY FIX—DOCTRINE TO FOLLOW

Stephanie K. Pell*

While the Jones *Court held unanimously that the Government's use of a GPS device to track Antoine Jones's vehicle for twenty-eight days was a Fourth Amendment search, the Justices disagreed on the facts and rationale supporting the holding. Beyond the very narrow trespass-based search theory regulating the Government's attachment of a GPS device to Jones's vehicle with the intent to gather information, the majority opinion does nothing to constrain government use of other tracking technologies, including cell phones, which merely involve the transmission of electronic signals without physical trespass. While the concurring opinions endorse application of the* Katz *reasonable expectation of privacy test to instances of government use of tracking technologies that do not depend on physical trespass, they offer little in the way of clear, concrete guidance to lower courts that would seek to apply* Katz *in such cases. Taken as a whole, then, the* Jones *opinions leave us still "*Jonesing*" for a privacy mandate. As of the writing of this Article, Congress has not been successful in passing legislation that would regulate government use of tracking technologies. A*

* Principal, SKP Strategies, LLC; Non-resident Fellow at Stanford Law School's Center for Internet and Society; former Counsel to the House Judiciary Committee; former Senior Counsel to the Deputy Attorney General, U.S. Department of Justice; former Counsel to the Assistant Attorney General, National Security Division, U.S. Department of Justice; and former Assistant U.S. Attorney, Southern District of Florida.

The author would like to thank Professor Anne Klinefelter and the *North Carolina Journal of Law & Technology* staff members for inviting me to participate in its Symposium on *U.S. v. Jones*: Defining a Search in the 21st Century (Jan. 25, 2013), and publish in the corresponding Symposium issue. The author would also like to thank Steven Bellovin, Jim Green, and Chris Soghoian for their feedback and assistance.

third regulator of government power has emerged, however, in the form of technology itself, specifically in new(ish) methods an individual or group of individuals can use to make it more difficult, in some cases perhaps impossible, for law enforcement to obtain the information it seeks. While waiting for more definitive action from the courts and Congress, such "privacy enhancing" anonymization and encryption technologies can provide a temporary "fix" to the problem of ever-expanding police powers in the digital age, insofar as they make law enforcement investigations more difficult and expensive, thereby forcing law enforcement to prioritize some investigations and, perhaps, de-emphasize or drop others. Moreover, at a time when cybersecurity is a national security priority and recommended "best practices" include the use of encryption technologies to protect, among other things, U.S. intellectual property, law enforcement is likely to face continued instances of "Going Dark" as it attempts to intercept communications in the face of the increasing availability and use of encryption technologies. As Congress considers possibilities for expanding law enforcement interception capabilities, it will be forced to accommodate the complex dualistic properties of technologies that, on one hand, bolster our national security against certain kind of threats while, on the other, they limit or thwart law enforcement's ability to fulfill its traditional public safety function of investigating crimes.

I. INTRODUCTION

> CHIEF JUSTICE ROBERTS: You think there would also not be a search if you put a GPS device on all of our cars, monitored our movements for a month? You think you're entitled to do that under your theory?
>
> MR. DREEBEN: The Justices of *this* Court?
>
> CHIEF JUSTICE ROBERTS: Yes.
>
> [. . .]
>
> MR DREEBEN: Under our theory and under this Court's cases, the Justices of this Court when driving on public roadways have no greater expectation of—

> CHIEF JUSTICE ROBERTS: So, your answer is yes, you could tomorrow decide that you put a GPS device on every one of our cars, follow us for a month; no problem under the Constitution?[1]

This exchange between the Chief Justice of the U.S. Supreme Court and Deputy Solicitor General Michael Dreeben occurred during the early part of the Government's oral argument in *United States v. Jones*.[2] Mr. Dreeben's answer, as it unfolded over the course of questioning by the Chief Justice and several other Justices, was essentially reducible to the proposition that, when the Government is monitoring the movements of any person in public (in this case on the public roadways), there is no constitutional impediment to tracking a car using a GPS device.[3] The argument relies on *United States v. Knotts*,[4] a case in which a radio transmitter beeper planted in a five gallon drum of chloroform emitted signals that assisted the Government in physically following an automobile carrying the drum on public streets,[5] where the Court held that "a person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another."[6] The Global Positioning System ("GPS") tracking technology at issue in *Jones*,

---

[1] Transcript of Oral Argument at 9–10, United States v. Jones, 132 S. Ct. 945 (2012) (No. 10-1259) (emphasis added), *available at* http://www.supremecourt.gov/oral_arguments/argument_transcripts/10-1259.pdf.

[2] 132 S. Ct. 945 (2012).

[3] Transcript of Oral Argument, *supra* note 1, at 9–22. Jones noted in his brief:

> GPS devices produce an accurate, continuous, and three-dimensional digital record of their position and velocity over any period of time—as well as that of any person or object carrying them. These data can be communicated to a remote computer through a cellphone connection and translated onto an interactive map.

Brief for Respondent Antoine Jones at 1, 10, *Jones*, 132 S. Ct. 945 (No. 10-1259) (citing Muhammad U. Iqbal & Samsung Lim, *Privacy Implications of Automated GPS Tracking and Profiling*, 29 IEEE TECH. & SOC'Y MAG., no. 2, 2010, at 39, *available at* http://www.gmat.unsw.edu.au/snap/publications/usman&lim2007c.pdf).

[4] 460 U.S. 276 (1980).

[5] *Id.* at 278.

[6] *Id.* at 281.

however, provided the Government with a far more powerful surveillance tool:

> For . . . four weeks, the GPS device calculated every movement and identified every stop Jones made in his vehicle every ten seconds of every day. Whenever the vehicle moved, the device generated location and velocity data; whenever the car was not moving, the device went into sleep mode and sent no data, thus informing law enforcement that the vehicle and device remained in place. Over the course of a month of virtually seamless GPS surveillance, the government obtained satellite-generated data not just about Jones's discrete journeys and stops, but also patterns of movement and location.[7]

For anyone in the audience[8] who had read the Government's opening brief in *Jones*, Mr. Dreeben's answer to the Chief Justice's question was not particularly surprising,[9] if palpably uncomfortable—imagine having to argue to the Supreme Court of the United States, on behalf of the entire Executive Branch, that there is no constitutional impediment to the Government's use of GPS devices to track their cars on public thoroughfares! It was a captivating moment, at once both humorous and dramatic: Chief Justice Roberts' hypothetical had threatened the logic of *Knotts* and put Dreeben, temporarily at least, on his heels. The question cut to the core issues before the Court by throwing into high relief law enforcement's unfettered, indiscriminate ability to track any individual's movements in public for days, weeks, even months at a time using a credit card sized GPS device discretely attached to the undercarriage of a car.[10] If there is little to no check (other than perhaps its better judgment) upon the Government's covert use of

---

[7] Brief for Respondent Antoine Jones, *supra* note 3, at 4 (internal citations omitted).

[8] The author was present in the audience at the *Jones* oral argument.

[9] *See* Brief for the United States at 12, United States v. Jones, 132 S. Ct. 945 (2012) (No. 10-1259) (relying on *Knotts* for the proposition that "technological enhancements in the ability to observe matters 'knowingly expose[d] to the public' do not render those observations a search").

[10] Chief Justice Roberts describes the GPS tracking technology at issue in Jones as giving law enforcement the ability to "just sit back in the station" and "push a button whenever they want to find out where the car is. They look at the data from a month and find out everywhere it's been in the past month." Transcript of Oral Argument, *supra* note 1, at 4.

GPS devices to monitor the comings and goings of Supreme Court Justices as they drive down public streets, what does that suggest about the lawful scope of the Government's ability to track the movements of regular citizens? Indeed, as Justice Sotomayor remarks, "The GPS technology [of] today is limited only by the cost of the instrument, which frankly right now is so small that it wouldn't take that much of a budget, local budget, to place a GPS [device] on every car in the nation."[11]

Likewise, Justice Breyer confronts the Deputy Solicitor General with his own concerns about the degree of government power enabled by unconstrained use of tracking technologies: "[W]hat would a democratic society look like if a large number of people did think that the government was tracking their every movement over long periods of time[?]"[12] Presumably in an effort to prevent this kind of harm, Justice Breyer announces he is searching for a "reason and principle" that would "reject" this kind of government surveillance "but wouldn't also reject [government tracking] 24 hours a day for 28 days,"[13] the period of surveillance at issue in *Jones*.[14]

Embedded in Justice Breyer's statements are several of the critical issues faced by the *Jones* Court. First, that modern day location tracking technologies, [15] beyond just the physical attachment of GPS tracking devices to cars at issue in *Jones*,[16] are enabling surveillance with a level of precision and on a scale heretofore unimaginable,[17] even in dystopian fiction.[18] True, the

---

[11] *Id.* at 25.

[12] *Id.* at 24.

[13] *Id.* at 25.

[14] United States v. Jones, 132 S. Ct. 945, 948 (2012) (No. 10-1259).

[15] *See infra* note 39.

[16] *See Jones*, 132 S. Ct. at 948 ("[A]gents installed a GPS tracking device on the undercarriage of the Jeep while it was parked in a public parking lot. Over the next 28 days, the Government used the device to track the vehicle's movements.").

[17] *See infra* note 39.

[18] Professor Lawrence Lessig observes that "while . . . analogies to Orwell [George Orwell's *1984*] are just about always useless," he makes one important

Court had acknowledged the potential for dragnet surveillance in *Knotts*,[19] but no more than that. In *Jones*, however, statements made by some of the Justices at oral argument,[20] along with elements of the concurrences,[21] evince the Court's general recognition that, despite the Government's protestations to the

---

comparison about the difference between today's technologies and the surveillance technologies in *1984*:

> While the ends of government in 1984 were certainly vastly more evil than anything our government would ever pursue, it is interesting to note just how inefficient, relative to the current range of technologies, Orwell's technologies were. The central device was a 'telescreen' that both broadcasted content and monitored behavior on the other side. But the great virtue of the telescreen was that you knew what it, in principle, could see. Winston knew where to hide, because the perspective of the telescreen was transparent. It was easy to know what it couldn't see, and hence easy to know where to do the stuff you didn't want to see. That's not the world we live in today. You can't know whether your search on the Internet is being monitored. You don't know whether a camera is trying to identify who you are. Your telephone doesn't make funny clicks as the NSA listens in . . . . The technologies of today have none of the integrity of the technologies of *1984*. None are decent enough to let you know when your life is being recorded.

LAWRENCE LESSIG, CODE 2.0 208–09 (Soho Books 2010); *see also* United States v. Cuevas-Perez, 640 F.3d 272 (7th Cir. 2011), a pre-*Jones* decision involving sixty hours of warrantless GPS tracking of the defendant's car by the Government, where Judge Wood observed that "[t]he technological devices available for such monitoring have rapidly attained a degree of accuracy that would have been unimaginable to an earlier generation. They make the system that George Orwell depicted in his famous novel, *1984*, seem clumsy and easily avoidable by comparison." *Id.* at 286 (Wood, J. dissenting).

[19] *Jones*, 132 S. Ct. 945 at n.6 (citing United States v. Knotts, 460 U.S. 276, 284 (1983)). ("*Knotts* noted the 'limited use which the government made of the signals from this particular beeper;' and reserved the question whether 'different constitutional principles may be applicable' to dragnet-type law enforcement practices' of the type made possible here, *ibid.*")

[20] See Justice Sotomayor's statement referencing the low cost of GPS surveillance that could permit the tracking of every car in the nation at *supra* note 11 and accompanying text. See also Chief Justice Robert's characterization of the Government's argument as allowing GPS tracking of individuals with no reason, suspicion, or limitation. Transcript of Oral Argument, *supra* note 1, at 15.

[21] *See* discussion *infra* Part II.

contrary,[22] we are now in a technological age where mass surveillance can and perhaps does occur.[23]

Second, Justice Breyer recognizes implicitly that such large-scale government surveillance can influence the behavior of individual citizens in a manner and on a scale that threatens the functioning of a democratic society. More than forty years ago, Vice President Hubert Humphrey had similarly observed that "[w]e act differently if we believe we are being observed. If we can never be sure whether or not we are being watched and listened to, all our actions will be altered and our very character will change."[24] Significantly, the iconic literary expression of a surveillance dystopia, Orwell's *1984*,[25] was referenced six times during the *Jones* oral argument.[26] Moreover, in her concurring opinion, Justice Sotomayor writes, "GPS monitoring—by making available at a relatively low cost such a substantial quantum of intimate information about any person whom the Government, in its unfettered discretion, chooses to track—may 'alter the relationship between citizen and government in a way that is inimical to democratic society.' "[27] Indeed, Justice Sotomayor not only recognizes the likely existence of mass surveillance, but also seems to be gesturing toward a theory of the resultant harm it could cause to our institutions in the form of a politically demoralized citizenry.

---

[22] During oral argument, Deputy Solicitor General Dreeben suggested that "the Court should address the so-called 1984 scenarios if they come to pass, rather using this case as a vehicle for doing so." Transcript of Oral Argument, *supra* note 1, at 25.

[23] *See* United States v. Garcia, 474 F.3d 994, 998 (7th Cir. 2007) ("The new [surveillance] technologies enable, as the old (because of expense) do not, wholesale surveillance. . . . Technological progress poses a threat to privacy by enabling an extent of surveillance that in earlier times would have been prohibitively expensive.").

[24] Hubert H. Humphrey, *Foreword* to EDWARD V. LONG, THE INTRUDERS viii (1967).

[25] GEORGE ORWELL, 1984 (Signet Classic 1990) (1949).

[26] *See* Transcript of Oral Argument, *supra* note 1, at 13, 25, 27, 33, 35, 57.

[27] United States v. Jones, 132 S. Ct. 945, 956 (2012) (Sotomayor, J., concurring) (quoting United States v. Cuevas-Perez, 640 F.3d 272, 285 (7th Cir. 2011) (Flaum, J., concurring)).

Third, Justice Breyer's statements illustrate a recognition that any rule or principle chosen to curb the Government's location tracking surveillance power must nevertheless account for law enforcement's need to investigate crimes.[28] Recognizing that some form of social harm is inherent in pervasive monitoring, Justice Breyer searches for a rule that would allow lawful government tracking short of such injurious mass surveillance, while nevertheless permitting the twenty-eight days of surveillance that occurred in *Jones* or, presumably, some shorter period of tracking.[29] Deputy Solicitor General Dreeben, however, warns against the "intolerable . . . line drawing problems" the Court could create through the language of its decision.[30] Indeed, this type of specific "line-drawing" does sound like work more appropriately left to the legislative process—at least an exasperated Justice Scalia seemed to conclude as much during oral argument when he exclaimed, more than rhetorically, "Don't we have any legislatures out there that could stop this stuff?"[31]

Ultimately, the *Jones* Court held unanimously that the Government's GPS tracking of the Jeep driven by Antoine Jones was a search under the Fourth Amendment.[32] As illustrated by the majority and two concurring opinions, however, the Justices are in disagreement with regard to both the facts and the rationale supporting this conclusion.[33] Indeed, if the Court's opinion in *Jones* is to be assessed as an attempt to create a clear rule or principle that sets appropriate limits on the Government's power to track the movements of its citizens with various types of location

---

[28] *See, e.g.*, Stephanie K. Pell & Christopher Soghoian, *Can You See Me Now?: Toward Reasonable Standards for Law Enforcement Access to Location Data That Congress Could Enact*, 27 BERKELEY TECH. L.J. 117, 151–56 (2012) (discussing how imposing a unitary probable cause standard for law enforcement access to all location data generated by cell phones can unduly limit law enforcement activities at early stages in an investigation).

[29] *See* Transcript of Oral Argument, *supra* note 1, at 13–15.

[30] *Id.* at 25.

[31] *Id.* at 26.

[32] *Jones*, 132 S. Ct. at 949 (affirming the judgment of the Court of Appeals for the D.C. Circuit with a 9-0 vote).

[33] *See* discussion *infra* Part II.

technologies, yet enables law enforcement to use such tracking tools effectively in its investigations, the decision must be seen as a noble failure.[34] In accordance with Justice Alito's concurring opinion and relevant scholarship, however, this Article presumes that this kind of *specific line drawing*—especially when it seeks to address the nuanced balancing of law enforcement, privacy and industry interests invoked by the Government's use of powerful and quickly evolving technologies to gain access to information[35]—is an effort that is best left to legislatures.[36] In stating this conclusion, however, this Article does not suggest that courts and the Fourth Amendment have no role to play with respect to protecting individuals from the unreasonable searches and seizures that may result from government use of new surveillance technologies. Rather, it proceeds with the implicit recognition that such Fourth Amendment protections will inevitably develop incrementally over time as courts attempt, with judicial, not legislative, tools, "to help restore the prior level of privacy protection" that existed before new technologies and social practices "ma[de] evidence substantially easier for the government to obtain."[37]

---

[34] *See, e.g.*, Pell & Soghoian, *supra* note 28, at 134–50 (discussing the lack of clarity and guidance offered by the *Jones* opinions with respect to legal standards governing law enforcement access to location data generated by cell phones and arguing that the Alito concurrence intensifies the confusion in the law surrounding current law enforcement access standards).

[35] *Id.* at 151 (arguing that in order to save courts from the "difficult acts of legal navigation" raised by determining the appropriate legal standards for law enforcement access to cell phone location data during the current pace of technological change, "policy makers should enact laws containing *clear* standards that strike the right balance among law enforcement needs and privacy and industry interests").

[36] *Jones*, 132 S. Ct. at 964 (Alito, J., concurring) ("In circumstances involving dramatic technological change, the best solutions to privacy concerns may be legislative." (citing Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 805–06 (2004) (arguing that Congress should be the primary driver of privacy protections when technology "is in flux"))).

[37] Orin S. Kerr, *An Equilibrium-Adjustment Theory of the Fourth Amendment*, 125 HARV. L. REV. 476, 480 (2011).

What *Jones* does offer, both through the arguments of the concurring opinions and a larger political message emanating from the very *lack* of controlling doctrine for any kind of location tracking that does not involve physical trespass, is a recognition that there is a need for a new privacy mandate that will respond adequately to the breadth of the Government's capacity, through the use of various location tracking technologies, "to ascertain, more or less at will [the] political and religious beliefs [and] sexual habits" of its citizens.[38] Indeed, the ambit of this recognition actually extends beyond the GPS tracking device at issue in *Jones* to other types of tracking or surveillance technologies and methods referenced in the case,[39] including Justice Sotomayor's questioning of the appropriateness of the third party doctrine for the digital age.[40] This doctrine stands for the premise that "an individual has no reasonable expectation of privacy in information voluntarily

[38] *Jones*, 132 S. Ct. at 956 (Sotomayor, J., concurring).

[39] *Id.* at 957 ("People disclose the phone numbers that they dial or text to their cellular providers; the URLs that they visit and the e-mail addresses with which they correspond to their Internet service providers; and the books, groceries, and medications they purchase to online retailers."); *id.* at 963 (Alito, J., concurring) ("In some locales, closed-circuit television video monitoring is becoming ubiquitous. On toll roads, automatic toll collection systems create a precise record of the movements of motorists who choose to make use of that convenience. Many motorists purchase cars that are equipped with devices that permit a central station to ascertain the car's location at any time so that roadside assistance may be provided if needed and the car may be found if it is stolen. Perhaps most significant, cell phones and other wireless devices now permit wireless carriers to track and record the location of users—and as of June 2011, it has been reported, there were more than 322 million wireless devices in use in the United States. For older phones, the accuracy of the location information depends on the density of the tower network, but new 'smart phones,' which are equipped with a GPS device, permit more precise tracking. For example, when a user activates the GPS on such a phone, a provider is able to monitor the phone's location and speed of movement and can then report back real-time traffic conditions after combining ('crowdsourcing') the speed of all such phones on any particular road. Similarly, phone-location-tracking services are offered as 'social' tools, allowing consumers to find (or to avoid) others who enroll in these services.").

[40] *Id.* at 957 (Sotomayor, J., concurring).

disclosed to third parties."[41] Perhaps more than any other single legal precedent, the third party doctrine facilitates warrantless government access to an ever-growing cache of information about individuals stored by third parties [42] who themselves have developed enormously sophisticated and accurate tracking technologies for commercial purposes.[43]

How such a mandate will take shape is not yet certain. For instance, how will courts and legislatures go about limiting the third party doctrine or otherwise curbing government surveillance powers post-*Jones*? Justice Scalia, as mentioned, points to the role of elected legislatures as crucial and implies that they have been lax in addressing the issues.[44] Indeed, Congress has made little progress towards providing clear rules that set appropriate limits on the Government's power to track the movements of its citizens with various types of location technologies.[45] But courts and legislatures are not the only parties to this process. Another player is taking the field in the form of *code* itself—that is, in the new(ish) technologies which limit the Government's ability to

---

[41] *Id.* (citing Smith v. Maryland, 442 U.S. 735, 742 (1979); United States v. Miller, 425 U.S. 435, 443 (1976)).

[42] *See generally* Stephanie K. Pell, *Systematic Access to Private Sector Data in the United States*, 2 INT'L DATA PRIVACY LAW, no. 4, 2012, at 247, *available at* http://idpl.oxfordjournals.org/cgi/reprint/ips020?ijkey=KkPfBFLbuMnUYsR&keytype=ref (discussing, for example, gaps in various statutory schemes enacted to create some level of privacy protection for third party data not afforded Fourth Amendment protection).

[43] Julie Angwin, *The Web's New Goldmine: Your Secrets*, WALL ST. J. (July 30, 2010), http://online.wsj.com/article/SB10001424052748703940904575395073512989404.html (discussing the fact that commercial consumer tracking technologies are getting smarter and more intrusive); *see also* Chris Jay Hoofnagle, Ashkan Soltani, Nathaniel Good, Dietrich J. Wambach & Mika D. Ayenson, *Behavioral Advertising: The Offer You Cannot Refuse*, 6 HARV. L. & POL' REV. 273 (2012) (explaining, for example, that "tailoring advertising—has become politically controversial because in order to pitch relevant advertising to individuals, companies have strong incentives to monitor individuals' use of the Internet pervasively and to build profiles of users").

[44] Transcript of Oral Argument, *supra* note 1, at 26; *see supra* Part I; *infra* Part IV.

[45] *See* discussion *infra* Part II.D.

access certain types of content and non-content communications, even when a Court has authorized the collection of such information.[46] These encryption and anonymization technologies offer their own form of implicit, incremental regulation insofar as they can prevent the Government from obtaining certain types of communications altogether or force the Government to get that information through far more labor intensive and expensive alternative methods.[47] By forcing the Government to try a little harder or spend a little more to obtain each unit of surveillance information, these technologies may reintroduce a needed measure of new friction into a digital age that has—for some time now—steadily facilitated law enforcement access to the point where it has arguably become too cheap and too easy.[48]

Part II of this Article discusses the three *Jones* opinions, summarizing some of their significant shortcomings and placing them within the context of the larger legal and policy debate about location tracking. Part II continues with an analysis of the *Jones* Court's call for a privacy mandate and its suggestions of how that mandate might emerge from its own future cases if a legislative solution is not found first, which is underscored both through the concerns expressed by Justices Sotomayor and Alito in their respective concurring opinions and through a larger political message emanating from the majority opinion's lack of doctrinal guidance. Part III, borrowing from Lawrence Lessig's contention

---

[46] *See* discussion *infra* Part III.

[47] *See id.*

[48] *See* United States v. Jones, 132 S. Ct. 945, 956 (2012) (Sotomayor, J., concurring) ("[B]ecause 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.' "); *see also* Christopher Soghoian, The Spies We Trust: Third Party Service Providers and Law Enforcement Surveillance (Aug. 2012) (unpublished Ph.D. dissertation, Department of Informatics, Indiana University), *available at* http://files.dubfire.net/csoghoian-dissertation-final-8-1-2012.pdf (explaining that "mass adoption of digital technologies over the past decade has led to a radical shift in the government's ability to engage in large scale surveillance").

that "code is law,"[49] discusses two specific encryption and anonymization technologies and describes how, for better or worse, they can make law enforcement's job harder, then goes on to place them within the context of the larger congressional public policy debate. Finally, Part IV concludes that, at least in the short run, these types of encryption and anonymization technologies promise a surer, quicker path or "fix" to certain aspects of the privacy mandate some are "*Jones*ing" for today.

II. MOSAICS, THIRD PARTIES, AND VERY TINY CONSTABLES

This Part first examines some of the limits of the majority opinion in *Jones*, as well as aspects of the *Jones* opinions that create particular challenges for lower courts, law enforcement, and industry with respect to determining the appropriate legal standards for law enforcement access to location data generated by cellular phones.[50] While the *Jones* facts did not involve law enforcement access to and use of cell phone location data,[51] the *Jones* opinions clearly illustrate the Justices' appreciation of the pending cell phone tracking issue, whether or not it can be resolved immediately by the Court.[52] Indeed, as this Part will discuss, the *Jones* decision arose during a still ongoing public policy debate before Congress over the appropriate standards for law enforcement access to location data.[53] Finally, this Part analyzes the call for action by some or multiple branches of government—found both in the concurring opinions and in the majority opinion's

---

[49] LESSIG, *supra* note 18, at 5; *see* discussion *infra* Part III.

[50] For an explanation of the various ways cell phones generate location data *see* Pell & Soghoian, *supra* note 28, at 126–33.

[51] The Government also obtained location data from Antoine Jones's cell phone and, having defeated Jones's motion to suppress evidence, intends to use it as evidence in a re-trial of Jones. United States v. Jones, No. 05-0386 (ESH), 2012 WL 6443136 (D.D.C. 2012); *see also* Suhrith Parthasarathy, *Federal Judge Allows Warrantless Use of Cell Phone Location Data, Thomson Reuters News & Insight*, THOMSON REUTERS (Dec. 19, 2012), http://newsandinsight.thomsonreuters.com/Legal/News/2012/12_-_December/Federal_judge_allows_warrantless_use_of_cell_phone_location_data/.

[52] *See* discussion *infra* Part II.D.

[53] *See* discussion *infra* Part II.D.

lack of doctrine addressing location tracking not involving physical trespass—for appropriate mechanisms to limit the Government's often unfettered access to information in the digital age.

A. *The Majority Opinion and Justice Alito's Concurrence*

In the *Jones* majority opinion authored by Justice Scalia, four other Justices [54] joined in holding that the "Government's installation of a GPS device on a target's vehicle, and its use of that device to monitor the vehicle's movements, constitutes a 'search.' "[55] Further defining the offending conduct, the majority opinion states, "The Government physically occupied private property for the purpose of obtaining information." [56] Consequently, though "[t]respass alone does not qualify [as a search]," a search does occur when it is "conjoined with . . . an attempt to find something or to obtain information."[57] The "key to the decision, [however,] is the predicate trespass" and, if such trespass occurs, "the fact that third parties can observe the vehicle is irrelevant."[58] Indeed, *Knotts* holds that information voluntarily conveyed to the public does not violate the *Katz*[59] reasonable expectation of privacy test [60] and thus does not render the Government's collection of such information a search. This conclusion is more or less still intact post-*Jones*,[61] since the *Jones*

---

[54] Roberts, Kennedy, Thomas, and Sotomayor joined.

[55] United States v. Jones, 132 S. Ct. 945, 949 (2012). The Court, however, did not decide whether the search was reasonable, and thus lawful, under the Fourth Amendment. *Id.* at 954. It therefore remains unclear as to whether a warrant is required for the Government's future use of GPS tracking devices.

[56] *Id.* at 949.

[57] *Id.* at 951 n.5.

[58] Christopher Slobogin, *Making the Most of* United States v. Jones *in a Surveillance Society: A Statutory Implementation of Mosaic Theory*, 8 DUKE J. OF CONST. L. & PUB. POL'Y (SPECIAL ISSUE) 2, 3 (2012).

[59] 389 U.S. 347 (1967).

[60] Kyllo v. United States, 533 U.S. 27, 33 (2001) ("As Justice Harlan's oft-quoted concurrence described it, a Fourth Amendment search occurs when the government violates a subjective expectation of privacy that society recognizes as reasonable." (citing United States v. Katz, 389 U.S. 347, 361 (1967))).

[61] *Jones*, 132 S. Ct at 951–52 ("We said that there has been no infringement of Knotts' reasonable expectation of privacy since the information obtained—the

majority opinion reconciles the two decisions by noting that the *Katz* test "*added to*, not *substituted for*, the common law trespassory test,"[62] while *Knotts* addressed the *Katz* test only.[63] Justice Scalia, while not repudiating the reasonable expectation of privacy test, reasoned that the Fourth Amendment must be interpreted to "assur[e] preservation of that degree of privacy that existed when the Fourth Amendment was adopted."[64] To accomplish a return to the status quo by preserving that particular degree of privacy, Justice Scalia "interpreted the Fourth Amendment as protecting against common law trespasses."[65] Accordingly, the Government's attachment of the GPS device with the intent to gather information was a common law trespass and, therefore, a Fourth Amendment search.[66]

Insofar as Jones's Fourth Amendment rights "did not rise or fall with the *Katz* formulation"[67] of what constitutes a search, the Court's trespass-based theory was a way to address the Government's unfettered ability to attach GPS tracking devices to cars and monitor movements on public roads without delving into how the Fourth Amendment might appropriately limit government use of other types of tracking technologies that solely employ the transmission of radio or other electronic signals not enabled by the Government's direct physical trespass—such as tracking a target's

---

location of the automobile carrying the container on public roads, and the location of the off-loaded container in open fields near Knotts' cabin—had been voluntarily conveyed to the public.")

[62] *Id.* at 952.

[63] *Id.* ("The holding in *Knotts* addressed only the former [*Katz* test], since the latter [trespass] was not at issue. The beeper had been placed in the container before it came into Knotts' possession, with the consent of the then-owner. Knotts did not challenge that installation, and we specifically declined to consider its effect on the Fourth Amendment analysis." (citations omitted)).

[64] *Id.* at 946 (quoting *Kyllo*, 533 U.S. at 34).

[65] Orin S. Kerr, *Defending Equilibrium-Adjustment*, 125 HARV. L. REV. F. 84, 88 (2012).

[66] *Id.* For a critique of the Majority's trespass analysis, see Peter A. Winn, *Trespass and the Fourth Amendment: Some Reflections on Jones*, USVJONES.COM (June 4, 2012), *available at* http://usvjones.com/2012/06/04/trespass-and-the-fourth-amendment-some-reflections-on-jones/.

[67] *Jones*, 132 S. Ct. at 950.

cell phone.[68] Indeed, Justice Alito criticizes the majority's trespass-based approach because, among other things:

> [It] largely disregards what is really important (the use of a GPS for 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).[69]

While Justice Alito agrees that the Court must ensure that individuals are afforded the same degree of privacy existing in or around 1789, he questions the majority's rather tenuous reliance on analogous eighteenth century situations to address this twenty-first century surveillance issue.[70] He humorously sketches the "very tiny constable" or "gigantic coach" necessary to permit the eighteenth century version of GPS tracking (that is, the constable hiding in the coach—unbeknownst to the occupants—to monitor its and their movements).[71]

In contrast to the pre-computer age, when significant privacy protections were more practical because the work of surveillance itself required more human labor, such as "a large team of agents, multiple vehicles, and perhaps aerial assistance,"[72] new technologies like GPS-enabled smart phones[73] and GPS tracking devices "make long-term monitoring relatively easy and cheap,"[74] thus increasing the Government's surveillance powers. In Justice Alito's view, society's expectation has been that law enforcement neither had nor could "secretly monitor and catalogue every single movement of an individual's car" over a long period of time.[75] Thus, under the *Katz* test, long-term monitoring, in this case four weeks of surveillance, was a Fourth Amendment search insofar as

---

[68] *Id.* at 953 ("Situations involving merely the transmission of electronic signals without trespass would remain subject to the *Katz* analysis.").
[69] *Id.* at 961 (Alito, J., concurring).
[70] *Id.* at 958.
[71] *Id.* at n.3.
[72] *Id.* at 963.
[73] *Id.* at 955 (Sotomayor, J., concurring).
[74] *Id.* at 964 (Alito, J., concurring).
[75] *Id.*

it "exceeded pre-GPS societal expectations that such invasive monitoring was" at least "unlikely," if not "impossible."[76]

In determining that four weeks of surveillance is a search, however, Justice Alito does not find it necessary to identify the precise point at which the GPS tracking becomes a search, but merely professes that the line was "surely crossed before the 4-week mark."[77] Moreover, Justice Alito writes that it is not necessary to consider whether long term tracking in investigations "involving extraordinary offenses" would violate the *Katz* test since he surmises that, in such significant cases, the Government has already engaged in long-term tracking with techniques that existed before GPS tracking was available.[78] His logic appears to suggest that, while perhaps with respect to some unnamed group of extraordinary offenses, societal expectations might contemplate the use of long-term tracking, no such expectation is commonly held with respect to investigations of most offenses.

The majority opinion takes Justice Alito to task on these issues, first for the proposition, which finds no precedent in the law, that the determination of whether a search occurs somehow depends on the type or nature of the crime being investigated.[79] Justice Scalia is equally critical of the line drawing problems that occur as a result of the rather arbitrary declaration that four weeks of GPS monitoring in a drug investigation is " 'surely' too long."[80] How does the Court make such determinations with, for example, two days of GPS tracking in a stolen electronics investigation or six months of monitoring a terrorism suspect?[81] Indeed, the majority opinion identifies one of the most "vexing problems"[82] inherent in Justice Alito's attempt to draw distinctions between short-term and long-term monitoring and apply them to the types of investigations where such electronic tracking techniques are used: the problem of

---

[76] Kerr, *supra* note 65, at 89.
[77] *Jones*, 132 S. Ct. at 964 (Alito, J., concurring).
[78] *Id.*
[79] *Id.* at 954 (majority opinion).
[80] *Id.*
[81] *Id.*
[82] *Id.*

finding an interpretive principle that enlists the Fourth Amendment in making such distinctions but avoids mere arbitrary line drawing. Even Justice Alito acknowledges that the best the Court can do in any case is "to apply existing Fourth Amendment doctrine and ask whether the use of GPS tracking in [that] particular case involved a degree of intrusion that a reasonable person would not have anticipated."[83] With this recognition, Justice Alito suggests that legislatures, not the judiciary, may be best suited to address privacy concerns arising from new technologies that expand government power.[84]

Justice Alito's exercise in line-drawing (or the lack thereof), premised on the theory that relatively short-term tracking comports with citizens' reasonable expectations of privacy whereas long-term tracking does not, is actually an attempt to introduce a new interpretive method into the Court's Fourth Amendment jurisprudence.[85] First introduced in the D.C. Circuit opinion *United States v. Maynard*,[86] Professor Orin Kerr calls this new approach the "mosaic theory."[87]

B. *The Mosaic Theory*

"At present, the mosaic theory is little more than a name,"[88] but it has the potential to be a disruptive element to Fourth Amendment doctrine. Prior to the Supreme Court's review in *Jones*, the *Maynard* court considered whether the Government's warrantless use of a GPS device placed on a vehicle to track a suspect's movements for twenty-eight days, twenty-four hours a day was an unreasonable search.[89] In concluding that the long-

[83] *Id.* at 964 (Alito, J., dissenting).
[84] *Id.*
[85] *See* Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311, 327 (2012).
[86] 615 F.3d 544 (D.C. Cir. 2010), *reh'g denied sub nom.* United States v. Jones, 625 F.3d 766 (D.C. Cir. 2010), *aff'd*, 132 S. Ct. 945 (2012).
[87] Kerr, *supra* note 85, at 313.
[88] Slobogin, *supra* note 58, at 4.
[89] *Maynard*, 615 F.3d at 555.

term GPS surveillance of movements exposed to public view was a search, the court explained:

> Prolonged surveillance reveals types of information not revealed by short term surveillance . . . [that] can each reveal more about a person than does any individual trip viewed in isolation . . . . A person who knows all of another's travels can deduce whether he is a weekly church goer, a heavy drinker, a regular at the gym, an unfaithful husband, an outpatient receiving medical treatment, an associate of particular individuals or political groups—and not just one such fact about a person, but all such facts.[90]

As Professor Kerr observes, under the mosaic theory, a court determines whether government conduct is a search "not by whether a particular individual act is a search, but rather whether an entire course of conduct, viewed collectively, amounts to a search."[91] Individual acts that may not, in their own right, be searches can become searches when committed in particular combinations.[92] For example, in *Maynard*, the court does not look at individual data records from the GPS device to determine whether individual trips are searches.[93] Instead, "the court looks at the entirety of surveillance over a one-month period and views it as one single 'thing' " subject to Fourth Amendment analysis.[94]

In an Article providing an exhaustive critique of the mosaic theory, Professor Kerr argues that the theory challenges the Supreme Court's established methods for analyzing when a Fourth Amendment search occurs and whether the search is reasonable.[95]

---

[90] *Id.* at 562.

[91] *See* Orin S. Kerr, *D.C. Circuit Introduces "Mosaic Theory" of Fourth Amendment, Holds GPS Monitoring a Fourth Amendment Search*, THE VOLOKH CONSPIRACY (Aug. 6, 2010, 2:46 PM), http://volokh.com/2010/08/06/d-c-circuit-introduces-mosaic-theory-of-fourth-amendmentholds-gps-monitoring-a-fourth-amendment-search/ (emphasis removed).

[92] *Id.*

[93] *Id.*

[94] *Id.*

[95] Kerr, *supra* note 85. This Article does not provide a full accounting of Professor Kerr's critique of the mosaic theory. Rather, it highlights particular elements of the critique that are useful to this Article's discussion of some of the practical problems the mosaic theory presents for courts, law enforcement, and defense attorneys.

He explains that, in determining when police action constitutes a Fourth Amendment search, courts have traditionally focused on "each 'particular governmental invasion of a citizen's personal security,' starting with the 'initial' step and then separately analyzing the 'subsequent' steps."[96] He calls this form of analysis the "sequential approach" and gives the example of an officer inserting a key into the door of a residence, opening the door, seeing an expensive piece of stereo equipment, moving the equipment to look at the serial number and then recording the serial number.[97] In this scenario, courts will analyze each particular outlined step as its "own Fourth Amendment event . . . evaluated independently of the others."[98]

The sequential approach also shapes the analysis of whether the search conduct is constitutionally reasonable.[99] Upon finding that a Fourth Amendment search has occurred, courts then evaluate whether the search is reasonable. There are two competing approaches for determining whether a search is reasonable. The traditional approach would only find a search to be reasonable when law enforcement has secured a warrant based on probable cause,[100] absent a special exception to the warrant requirement.[101] More recently, however, the Court has suggested a different approach: "Reasonableness now is understood as requiring a balancing of interests: courts consider whether the government interests advanced by the use of an investigatory technique

---

[96] *Id.* at 316 (citing United States v. Dionisio, 410 U.S. 1, 8–9 (1973)).

[97] *Id.* at 315–16.

[98] *Id.* at 316.

[99] *Id.* at 317–18.

[100] *See* FED. R. CRIM. P. 41(c) (listing categories of probable cause: "(1) evidence of a crime; (2) contraband, fruits of crime, or other items illegally possessed; (3) property designed for use, intended for use, or used in committing a crime; or (4) a person to be arrested or a person who is unlawfully restrained").

[101] Kerr, *supra* note 85, at 318 (citing United States v. Jeffers, 342 U.S. 48, 51 (1951) ("Over and again this Court has emphasized that the mandate of the Amendment requires adherence to judicial processes. Only where incident to a valid arrest, or in 'exceptional circumstances,' may an exemption lie, and then the burden is on those seeking the exemption to show the need for it." (citations omitted) (quoting Johnson v. United States, 333 U.S. 10, 14–15 (1948)))).

outweigh the privacy interest that its use threatens."[102] This balancing approach can result in the requirement of a warrant, some lesser form of regulation, or perhaps no regulation at all.[103] But under both approaches, "reasonableness rest[s] on the assumption that searches are readily identifiable acts that occur over readily identifiable periods of time."[104]

It is not hard to appreciate that the mosaic theory—which looks not at single acts, but which aggregates an entire course of conduct—has the potential to wreak havoc on the process by which courts determine whether a search has occurred and, if it has, whether it was reasonable. At what point and on what basis should a court determine, for instance, that a single act or series of acts amount to the prolonged surveillance that triggers the mosaic theory? And how does a prosecutor, judge or defense attorney recognize the phenomenon? Moreover, investigations proceed over time, unfolding sequentially like narrative fiction. As such, once begun, they are simultaneously prospective and retrospective, with each new fact having the potential both to refine the direction of the investigation's forward course and correct previous

---

[102] *Id.* (citing United States v. Place, 462 U.S. 696, 703 (1983) ("We must balance the nature and quality of the intrusion on the individual's Fourth Amendment interests against the importance of the governmental interests alleged to justify the intrusion.")); *see also* Sampson v. California 547 U.S. 843, 848 (2006) (" [U]nder our general Fourth Amendment approach we examin[e] the totality of the circumstances to determine whether a search is reasonable within the meaning of the Fourth Amendment."); Kerr, *supra* note 85, at 318. Whether a search is reasonable "is determined by assessing, on the one hand, the degree to which it intrudes upon an individual's privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests." *Id.* at 318–19 (internal quotation marks omitted).

[103] Kerr, supra note 85, at 318 (citing *Sampson*, 547 U.S. at 848).

[104] *Id.* at 318–19. Professor Kerr also argues that the sequential approach "forms the foundation of the warrant requirement" insofar as the Fourth Amendment's warrant clause has a particularity requirement that limits searches by requiring that they occur at a particular place and that the Government's searches for specific types of evidence, all that must be identified in the warrant. *Id.* at 319. The sequential approach has "obvious force" because the particularity requirement is "premise[d]" on the fact that "searches are discrete things that can occur in discrete places to find discrete items." *Id.*

erroneous assumptions. How would the mosaic theory regulate the integration of several investigative techniques, each of which individually might not constitute a search but which nevertheless could, when aggregated together with other techniques, help create the kind of intimate picture of a person's life that the *Maynard* court sought to protect from undue scrutiny?[105] Accordingly, the Solicitor General has argued in the Government's *Jones* brief that "the 'mosaic' theory is unworkable. Law enforcement officers could not predict when their observations of public movements would yield a larger pattern and convert legitimate short-term surveillance into a search. Courts would be hard pressed to pinpoint that moment, even in retrospect."[106]

Notwithstanding the problematic implications of the mosaic theory, the concurring opinions in *Jones* suggest that, in some future case, there may be five votes for a mosaic-type Fourth Amendment theory holding that "the use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy."[107] While Justice Sotomayor did not join

---

[105] *See* United States v. Maynard, 615 F.3d 544, 562 (D.C. Cir. 2010) ("Prolonged surveillance reveals types of information not revealed by short-term surveillance, such as what a person does repeatedly, what he does not do, and what he does ensemble. These types of information can each reveal more about a person than does any individual trip viewed in isolation. Repeated visits to a church, a gym, a bar, or a bookie tell a story not told by any single visit, as does one's not visiting any of these places over the course of a month. The sequence of a person's movements can reveal still more; a single trip to a gynecologist's office tells little about a woman, but that trip followed a few weeks later by a visit to a baby supply store tells a different story. A person who knows all of another's travels can deduce whether he is a weekly church goer, a heavy drinker, a regular at the gym, an unfaithful husband, an outpatient receiving medical treatment, an associate of particular individuals or political groups—and not just one such fact about a person, but all such facts." (internal citations omitted)).

[106] Brief for the United States at 14, United States v. Jones, 132 S. Ct. 945 (2012) (No. 10-1259). Indeed, Respondent Jones did not employ the *Maynard* "mosaic theory" in his brief to the Supreme Court. *See* Brief for Respondent Antoine Jones, *supra* note 3, at 45.

[107] *Jones*, 132 S. Ct. at 964 (Alito, J., concurring). Justices Ginsburg, Breyer, and Kagan joined Justice Alito's concurrence. *See id.*

the Alito concurrence, in her own she states, "I agree with Justice Alito that, at the very least, 'longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy.' "[108]

C. *A Call for a New Privacy Mandate*

Justice Sotomayor joined the *Jones* majority opinion, not the Alito concurrence.[109] In doing so, she writes that "the majority's opinion reflects an irreducible constitutional minimum: When the Government physically invades personal property to gather information, a search occurs."[110] For her, "The reaffirmation of that principle suffices to decide this case."[111] But her support for the opinion, which (merely) affirms the "constitutional relevance" of the Government's physical trespass on private property,[112] does not end her analysis of the privacy interests and expectations at issue with respect to other forms of government surveillance that do not require such physical intrusion.[113] Indeed, she notes that Justice Alito is correct in observing that nontrespassory surveillance techniques will "affect the *Katz* test by shaping the evolution of societal privacy expectations."[114] She therefore agrees that, "*at the very least*, 'longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy.' "[115]

Having qualified the two other *Jones* opinions as, more or less, addressing constitutional minimums, Justice Sotomayor ventures further to suggest that, in investigations employing "even short-

---

[108] *Id.* at 955 (Sotomayor, J., concurring).

[109] *See supra* note 54 and *infra* note 112.

[110] *Jones*, 132 S. Ct at 955 (Sotomayor, J., concurring).

[111] *Id.*

[112] *Id.* Indeed, Justice Sotomayor criticizes the Alito concurrence for "discount[ing] altogether the constitutional relevance of the Government's physical intrusion on Jones' Jeep," thereby "erod[ing] that longstanding protection for privacy expectations inherent in items of property that people possess or control." *Id.*

[113] *Id.*

[114] *Id.*

[115] *Id.* (emphasis added).

term monitoring, some unique attributes of GPS surveillance relevant to the *Katz* analysis will require particular attention."[116] For her, the privacy interests at issue with GPS monitoring include the Government's ability to ascertain "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."[117] She also recognizes that once recorded and stored, the Government can "mine" such information, perhaps for that person's lifetime and beyond.[118] Indeed, depending on time frames of storage,[119] it may become impossible to ever escape one's past. Moreover, she asserts that because government use of GPS monitoring is surreptitious and "cheap" when compared with other traditional methods of surveillance, it evades some of the "checks" or sources of friction in the system that "constrain

---

[116] *Id.*

[117] *Id.*

[118] *Id.* at 956.

[119] Consider the congressional testimony of Professor Matt Blaze given in response to a question posed by Rep. Jerrold Nadler (D-NY) about data retention practices of mobile service providers:

> Mr. NADLER. [. . .] What is the technological necessity and what is the practice of retaining this information? In other words they need to know where you are now so they can route the call. Do they need to know where you were an hour ago or a day ago? And do they retain this information? And if so, why?
>
> Mr. BLAZE. Well, every service provider—I should say I am not speaking for any service provider, and every service provider will have its own practices—but in general, service providers record everything essentially forever. This information is extraordinarily valuable for business, marketing and technical purposes. It tells them where their network needs to be improved, were dead spots are, and how their customers use their phones.

ECPA Reform and the Revolution in Location Based Technologies and Services: Hearing Before the Subcomm. on the Constitution, Civil Rights, and Civil Liberties of the H. Comm. on the Judiciary, 111th Cong. 16 (2010) [hereinafter *ECPA Reform Hearing*], *available at* http://judiciary.house.gov/hearings/printers/111th/111-109_57082.pdf.

abusive law enforcement practices: limited police resources and community hostility."[120]

Justice Sotomayor's succinct analysis of the privacy implications of GPS monitoring, which encompasses location tracking beyond the physical attachment of GPS devices, highlights some of the most significant privacy concerns in the digital age: data mining,[121] the relative strength of access standards, data acquisition practices so cheap and easy they can facilitate abusive police activities,[122] and a limitless flow of third party data law enforcement can use to expose or reconstruct the intimate details of a person's life.[123] Indeed, Justice Sotomayor warns that such cheap, unfettered access to broad swaths of intimate information "may alter the relationship between citizen and government in a way that is inimical to democratic society."[124] For her, then, such technology, which is generating the Government's increasingly clear sense of sight with regard to the lives of individuals, facilitates a power shift that is fundamentally inhibitory to open participation in a democratic society.

Drawing on the work of several scholars, Professor Paul Ohm argues that the fundamental goals of the Fourth Amendment should be limiting government power and preserving each citizen's

---

[120] *Jones*, 132 S. Ct. at 956 (Sotomayor, J., concurring) (quoting Illinois v. Lidster, 540 U.S. 419, 426 (2004)).

[121] *See* Fred H. Cate, *Government Data Mining: The Need for a Legal Framework*, 43 HARV. C.R.-C.L. L. REV. 435 (2008) (describing the large volume and variety of personal data to which the Government has access and examining the absence of any meaningful limits on that access).

[122] *See* Pell, *supra* note 42 (discussing gaps in various privacy statutes and government practices which, for example, facilitated the FBI's abuse of national security letters).

[123] *See* Paul Ohm, *The Fourth Amendment In A World Without Privacy*, 81 MISS. L.J. 1309, 1318–21 (2012) (describing four technological trends "which enable a powerful, new surveillance society" and arguing that such trends are facilitating law enforcement's "shift from being active producers of surveillance to passive consumers, essentially outsource all of their surveillance activities to private third parties").

[124] *Jones*, 132 S. Ct. at 956 (Sotomayor, J., concurring) (quoting United States v. Cuevas-Perez, 640 F.3d 272, 285 (7th Cir. 2011) (Flaum, J., concurring)).

liberty.[125] Indeed, he asserts that the Fourth Amendment was "originally intended and is better interpreted to ensure not privacy, but liberty from undue government power."[126] In support of this argument, Professor Ohm draws from the work of some constitutional scholars who employ an originalist interpretive frame—that the Fourth Amendment was meant to protect colonists from the Crown's use of general warrants, which entitled British troops to search indiscriminately and without suspicion.[127] In the digital age, law enforcement is relying more and more on "private surveillance,"[128] that is, upon data held by non-government third parties, to fuel its investigations.[129] A great deal of such data is shielded from Fourth Amendment protection because we have no reasonable expectation of privacy in information voluntarily disclosed to third parties.[130] Professor Ohm predicts that, ultimately, law enforcement "will shift their time, energy, and money away from self-help policing [and] becom[e] passive consumers rather than active producers of surveillance."[131] Accordingly, the *Katz* reasonable expectation of privacy test will continue to become less relevant for purposes of implementing

---

[125] Paul Ohm, *Three Fixes for the Fourth Amendment after Jones*, USVJONES.COM (June 2, 2012), http://usvjones.com/2012/06/02/three-fixes-for-the-fourth-amendment-after-jones/#more-152 (citing DANIEL SOLOVE, NOTHING TO HIDE 114 (2011); *see also* Morgan Cloud, *The Fourth Amendment During the* Lochner *Era: Privacy, Property, and Liberty in Constitutional Theory*, 48 STAN. L. REV. 555, 618–19 (1996)); Thomas P. Crocker, *From Privacy to Liberty: The Fourth Amendment After* Lawrence, 57 UCLA L. REV. 1, 56 (2009); Jed Rubenfeld, *The End of Privacy*, 61 STAN. L. REV. 101, 104 (2008); William J. Stuntz, *The Substantive Origins of Criminal Procedure*, 105 YALE L.J. 393, 446 (1995);.

[126] Ohm, *supra* note 123, at 1311–12.

[127] *Id.* at 1334 (citing Morgan Cloud, *Pragmatism, Positivism, and Principles in Fourth Amendment Theory*, 41 UCLA L. REV. 199, 296–97 (1993)).

[128] Ohm, *supra* note 125.

[129] *See id.*

[130] *See* Smith v. Maryland, 442 U.S. 735 (1979); United States v Miller, 425 U.S. 435 (1976).

[131] Ohm, *supra* note 125.

Fourth Amendment protections in the digital age.[132] Indeed, Professor Ohm suggests that the Fourth Amendment already exists in world without privacy, so what is left for *Katz* to protect?[133] He therefore calls for a "shift away from Katz's reasonable expectation of privacy to rules that focus instead on the balance of power between the police and the people."[134]

Notwithstanding the fact that Justice Sotomayor appears to focus on the *Katz* test for purposes of examining and curbing the expanded government power afforded by GPS tracking technologies,[135] she suggests that, "More fundamentally, it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties."[136] She notes that "[p]eople disclose the phone numbers that they dial or text to their cellular providers; the URLs that they visit and the e-mail addresses with which they correspond to their Internet service providers; and the books, groceries, and medications they purchase to online retailers."[137] Cognizant of the fact that the Fourth Amendment provides little to no limit on government acquisition of this information, she is skeptical of Justice Alito's observance that people may find the "tradeoff of privacy for convenience worthwhile" (e.g., we willingly generate more constitutionally non-protected third party data for the convenience of mobile devices) and that we have come to accept this "diminution of privacy as inevitable."[138] On the contrary, she suggests that this "trade" is not self-conscious and informed in a manner that could support his conclusions.[139] As such, she does not accept either the conclusions themselves or the

---

[132] Ohm, *supra* note 123, at 1336–39 ("[T]he age of using privacy as a measuring stick for Fourth Amendment protection is likely soon to draw to a close.").

[133] *Id.* at 1334.

[134] *Id.* at 1334–35.

[135] United States v. Jones, 132 S. Ct. 945, 955–56 (2012) (Sotomayor, J., concurring).

[136] *Id.* at 957.

[137] *Id.*

[138] *Id.*

[139] *Id.*

general idea of "treat[ing] secrecy as a prerequisite for privacy" for purposes of receiving Fourth Amendment protections.[140]

Professor Ohm describes this phenomenon as "mark[ing] the beginning of the end of the third party doctrine."[141] Perhaps more importantly, he writes that the Sotomayor concurrence "begins to embrace the move away from privacy to power and liberty."[142] But how such a move will further materialize remains to be seen. Will the Court move away from or supplement the *Katz* test?[143] Will it revisit *Knotts*?[144] Will it reexamine and limit the third party doctrine? One thing seems relatively certain: None of these possible changes or additions to Fourth Amendment doctrine will happen quickly.[145]

D. *The Political Message of* Jones *and the Larger Public Policy Debate*

The Court's unanimous holding that the Government's installation of a GPS device on Antoine Jones's Jeep and subsequent tracking of his vehicle for twenty-eight days was a search should first be understood as a win for the respondent.[146] That result, or some tally of votes which would have overturned Jones's conviction, no matter how the Court found its way there, was, of course, the duty and primary goal of his counsel.[147]

---

[140] *Id.*

[141] Ohm, *supra* note 125.

[142] *Id.*

[143] *See supra* note 60.

[144] *See supra* Part I and accompanying notes.

[145] *See* Susan Freiwald, *The* Davis *Good Faith Rule and Getting Answers to the Questions* Jones *Left Open*, 14 N.C. J.L. & TECH. 341 (observing that the Supreme Court has not addressed location tracking since the Knotts and Karo cases from the 1980s and explaining that "[a] review of lower court decisions in the wake of Jones reveals that, rather than beginning to answer the questions *Jones* left open, courts are largely avoiding substantive Fourth Amendment analysis of location data privacy").

[146] Walter Dellinger, Keynote Address at the *North Carolina Journal of Law & Technology* Symposium: *U.S. v. Jones*: Defining a Search in the 21st Century (Jan. 25, 2013), *available at* http://ncjolt.org/multimedia/symposium-videos.

[147] *Id.*

Beyond this immediate win, it is hard not to interpret the unanimous vote as the Court's unequivocal repudiation of the unfettered, indiscriminate tracking that the Government asserted was constitutionally permissible when using a GPS device to monitor movements on public roadways. The Court, however, held back on delivering a majority opinion that constrains government use of tracking technologies that do not depend on physical trespass—like cell phones or tablets.[148] One can speculate as to why it did not venture into this territory. The simple answer may be, as Justice Scalia and Justice Sotomayor both suggest, the facts before the Court did not require it to resolve some of the "vexing problems" that location tracking—absent physical trespass—present.[149]

Such "vexing problems" left open by *Jones* majority are, however, pressing issues for lower courts, as well as the Executive and Legislative branches of government.[150] Moreover, the political message emanating from the *lack* of controlling doctrine with respect to location tracking that does not involve physical trespass should not be discounted as merely a question left unanswered by the Court in *Jones*. Indeed, "unanswered" should not be interpreted to mean "unaddressed" altogether, since the very threat

---

[148] United States v. Jones, 132 S. Ct. 945, 953 (2012) ("Situations involving merely the transmission of electronic signals without trespass would remain subject to the *Katz* analysis.").

[149] *Id.* at 954 ("We may have to grapple with these 'vexing problems' in some future case where a classic trespassory search is not involved and resort must be had to *Katz* analysis; but there is no reason for rushing forward to resolve them here."); *id.* at 955 (Sotomayor, J., concurring) ("[T]he trespassory test applied in the majority's opinion reflects an irreducible constitutional minimum: When the Government physically invades personal property to gather information, a search occurs. The reaffirmation of that principle suffices to decide this case.").

[150] *See* Pell & Soghoian, *supra* note 28 (describing how the legal mystery surrounding the proper law enforcement access standard for prospective and historical location data remains unsolved which has created, along with conflicting rulings over the appropriate law enforcement access standard for both prospective and historical location data, a messy, inconsistent legal landscape where even judges in the same district may require law enforcement to meet different standards before authorizing law enforcement to compel location data).

of doctrine to follow—perhaps some formulation of the mosaic theory—is arguably a powerful signal to law enforcement that it must make its own efforts to resolve the prevailing uncertainty, whether through internal self-scrutiny or earnest participation in the legislative process. In the wake of *Jones*, for example, the FBI General Counsel expressed the difficulty government lawyers now face in providing guidance to law enforcement officers with respect to the type of legal process needed to compel or acquire various types of location data or execute other law enforcement techniques in the course of criminal investigations.[151] This lack of clarity, which forces law enforcement to question the legal standards permitting access to various types of location data can, among other things, disrupt the progress of investigations and make the prudent prosecutor worry about whether her evidence will be admissible at trial. Indeed, after the *Jones* decision came down, federal law enforcement agents were instructed to turn off three thousand GPS devices while government lawyers searched for an appropriate legal theory to permit them to be reactivated so, at a minimum, they could be located and retrieved.[152] Moreover, the FBI General Counsel has described the difficulty with providing comprehensive, accurate guidance that would attempt to instruct law enforcement agents on how to conduct activities in anticipation of five potential future votes for some form of the mosaic theory.[153]

---

[151] *See* Julia Angwin, *FBI Turns Off Thousands of GPS Devices After Supreme Court Ruling*, WALL ST. J. (Feb. 25, 2012, 3:36 PM), http://blogs.wsj.com/digits/2012/02/25/fbi-turns-off-thousands-of-gps-devices-after-supreme-court-ruling/ ("For instance, . . . [the FBI General explained that the] agency is now 'wrestling' with the legality of whether agents can lift up the lid of a trash can without committing trespass.").

[152] *Id.* The FBI General Counsel explained that "[a]fter the ruling [in *Jones*], the FBI had a problem collecting the devices that it had turned off. . . . In some cases, . . . the FBI sought court orders to obtain permission to turn the devices on briefly—only in order to locate and retrieve them." *Id.*

[153] *Id.* ("The agency is also considering the implications of the concurring justices—whose arguments were largely based on the idea that a person has a reasonable expectation of privacy in the totality of their movements, even if those movements are in public. 'From a law enforcement perspective, even

While both Justices Scalia and Alito have directly given some indication that Congress is the better branch of government to address expanded government power afforded by location tracking technologies,[154] as of the writing of this Article, Congress has not fared any better at creating clear rules that account appropriately for this expanded power without unduly limiting law enforcement investigations.[155] Congress has made some initial fitful progress, if progress can be measured by hearings held[156] or bills drafted, which set new standards for law enforcement compelled disclosures of location data from third parties and the use of GPS tracking devices placed on cars.[157] But Congress has its own substantive challenges with respect to addressing the expansion of government power enabled by new and evolving surveillance technologies. If courts are generally limited by the very specificity of their mission under the Constitution in applying existing Fourth Amendment doctrine to the facts of a particular case, as Justice Alito would prescribe,[158] then Congress must confront the inverse

---

though it's not technically holding, we have to anticipate how it's going to go down the road.' "). At the conference where these statements were made, the FBI General Counsel held up thick draft memos to underscore his point that the *Jones* Court had created a great deal of difficulty with respect to providing clear, accurate guidance to the field. *University of San Francisco Law Review* Symposium: Big Brother in the 21st Century? Reforming the Electronic Communications Privacy Act (Feb. 24, 2012). The author was in the audience during the General Counsel's remarks.

[154] *See supra* Part I; United States v. Jones, 132 S. Ct. 945, 964 (2012) (Alito, J., concurring).

[155] *See* Pell & Soghoian, *supra* note 28, at 157–62 (discussing various challenges Congress faces in passing legislation to regulate law enforcement access to location data).

[156] *See, e.g.*, *ECPA Reform Hearing*, *supra* note 119; *Hearing on H.R. 2168, the "Geolocational Privacy and Surveillance Act," Before the Subcomm. on Crime, Terrorism and Homeland Security of the H. Comm. on the Judiciary*, 112th Cong. (2012).

[157] *See, e.g.*, Online Communications and Geolocational Protection Act, H.R. 983, 113th Cong. (2013); Geolocational Privacy and Surveillance Act, H.R. 2168, 112th Cong. (2011); Geolocational Privacy and Surveillance Act, S. 1212, 112th Cong. (2011);. These bills require a Rule 41 "probable cause" standard for all law enforcement compelled disclosures of cell phone location data.

[158] *See supra* discussion in Part II.A.

challenge of the potentially grand scope of its own inquiry. That is, ideally, Congress should examine the issues broadly (to include understanding how the technology works so as to appreciate how it impinges on privacy interests and expands or limits government power), evaluate the positions of the various stakeholders (which, in the case of electronic surveillance, often involves conflicting but deeply held positions concerning privacy, law enforcement and industry equities),[159] and craft more nuanced compromises (which can and probably should include privacy protections beyond simple tightening of law enforcement access standards)[160] than a court would likely derive through a discrete application of the Fourth Amendment.[161]

An earlier article co-authored by this writer and Dr. Christopher Soghoian directly examines the dynamics of the policy debate currently taking place over law enforcement access to cell phone location data and some of the substantive challenges facing Congress with respect to finding reasonable standards for law enforcement location data acquisition.[162] It argues that the dueling policy positions taken by two of the three major stakeholders (privacy advocates and law enforcement) have resulted in a stalemate that has stifled Congress's ability to pass legislation that would raise some additional degree of privacy protection against law enforcement access to location data.[163] Privacy advocates are seeking legislation that would require law enforcement to obtain a warrant based on probable cause to access any amount (even a single point of location data representing where someone was at one moment in time) and duration of location data, including both historical (where someone was) and prospective (real-time,

---

[159] *See* Pell & Soghoian, *supra* note 28, at 124–25 (generally describing the conflicting positions law enforcement and privacy advocates have taken with respect to standards permitting law enforcement access to location data).

[160] *Id.* at 176–77 (arguing that access standards alone will not achieve the appropriate balance between law enforcement, privacy and industry equities).

[161] *See* Slobogin, *supra* note 58 (proposing a statutory implementation of the mosaic theory).

[162] *See* Pell & Soghoian, *supra* note 28.

[163] *Id.* at 123–24.

forward-looking tracking).[164] One measure of the effectiveness of that advocacy is the introduction of several bills that adopt an "all warrant" standard.[165] Such "warrant only" bills, however, are unlikely to become law because law enforcement makes compelling arguments that a blanket warrant standard would unduly impede legitimate law enforcement investigative activities, especially at early stages of an investigation when police or federal agents are unlikely to be able to demonstrate that there is probable cause to believe that the location data itself is evidence of a crime.[166]

Just as Justice Breyer, during the *Jones* oral argument, announced that he was searching for a "reason and [a] principle" that would "reject" this kind of government surveillance "but wouldn't also reject [government tracking] 24 hours a day for 28 days,"[167] Congress continues to search for the correct balance. But even if law enforcement advocacy is ultimately successful in preventing legislation that codifies a blanket warrant standard for all types of location tracking, the *Jones* opinions may be a catalyst for the Department of Justice ("DOJ") and state and local law enforcement to begin earnestly engaging with Congress in an effort to agree on some reasonable privacy protections. Indeed, Justice Alito's answer for how to deal with the thorny line drawing problem under a theory that does not define when the mosaic materializes is simple: "[W]here uncertainty exists with respect to whether a certain period GPS surveillance is long enough to constitute a Fourth Amendment Search, the police may seek a warrant."[168] If this potential reality is unworkable (that is, if an all warrant standard for any form location tracking will unduly limit

---

[164] *Id.* at 123.

[165] *See supra* note 157.

[166] Pell & Soghoian, *supra* note 28, at 154–56 (explaining how a "strict probable cause standard for the disclosure of location information could interfere with legitimate law enforcement objectives").

[167] Transcript of Oral Argument, *supra* note 1, at 25.

[168] United States v. Jones, 132 S. Ct. 945, 964 (2012) (Alito, J., concurring).

investigative activities),[169] or if the prospects of providing guidance to the field agents in the wake of the *Jones* opinions, which suggest there may be five votes for a mosaic-like Fourth Amendment theory, is too challenging,[170] then law enforcement can avail itself of the congressional balancing process.

III. TECHNOLOGY GIVES AND TECHNOLOGY TAKES AWAY

The Supreme Court in *Jones* and the Congress, each within the scope of its respective authority, are searching for the appropriate way to regulate government use of location tracking technologies. Moreover, Justice Sotomayor, in her concurrence, also seeks to curb overly broad government access to other types of data, the collection of which has the effect of magnifying the Government's power by sharpening the acuity of its tenacious gaze—a tendency she suggests could unreasonably and harmfully inhibit citizen participation in a democratic society.[171] But the courts and Congress are not the only possible influences upon the scope and manner of government access to information. Indeed, there is a third player on the field who can act as an indirect regulator of government surveillance powers and who can, in doing so, change the very facts and circumstances Congress and the courts must accommodate in their own more direct efforts to intervene. This third regulator is technology itself in the form of specific new(ish) methods an individual or group of individuals can use to make it more difficult, in some cases perhaps impossible, for law enforcement to obtain the information it seeks.

Professor Lawrence Lessig has written about code as the "salient regulator" of cyberspace, summarizing the concept in the now common aphorism, "code is law."[172] He explains:

---

[169] *See* Transcript of Oral Argument, *supra* note 1, at 17. Deputy Solicitor General Dreeben made statements at the *Jones* oral argument indicating that the "principle use" of GPS tracking surveillance "is when police have not yet acquired probable cause but have a situation that does call for monitoring."

[170] *See* discussion *supra* note 153.

[171] *Jones*, 132 S. Ct. at 956 (Sotomayor, J., concurring); *see also supra* Part II.

[172] LESSIG, *supra* note 18, at 5.

> This regulator is code—the software and hardware that make cyberspace as it is. This code, or architecture, sets the terms on which life in cyberspace is experienced. It determines how easy it is to protect privacy, or how easy it is to censor speech. It determines whether access to information is general or whether information is zoned. It affects who sees what, or what is monitored.[173]

Professor Lessig's general maxim about cyberspace, "code as regulator, code is law," is useful to explain a third set of forces, including encryption and anonymization technologies (two components of a broader set of privacy enhancing technologies).[174] These technologies may prove to be additional, perhaps more effective, mechanisms for maintaining reasonable limits upon the rapid increase of government power that is a leading characteristic of the digital age, in which the acuity of both the Government's own gaze and that of the commercial third parties who often cooperate with it has grown immeasurably sharper.[175] Technology giveth, and technology taketh away. Indeed, this Part argues that these technologies can "give" significantly by playing dual privacy- and security-enhancing roles in providing, for example, defenses against cybersecurity threats, while they simultaneously "take away" in similar measure by limiting or preventing law enforcement access to communications content.[176] One of these technologies can also allow people to browse and communicate over the Internet anonymously, thus facilitating the protection of

---

[173] Lawrence Lessig, *Code Is Law*, HARV. MAG., Jan.–Feb. 2000, *available at* http://harvardmagazine.com/2000/01/code-is-law-html.

[174] *See* ENTERPRISE PRIVACY GROUP, PRIVACY BY DESIGN: AN OVERVIEW OF PRIVACY ENHANCING TECHNOLOGIES 2 (2008), *available at* http://www.ico.org.uk/upload/documents/pdb_report_html/pbd_pets_paper.pdf ("There is no widely accepted definition for the term Privacy Enhancing Technologies (PETs) although most encapsulate similar principles; a PET is something that: 1. reduces or eliminates the risk of contravening privacy principles and legislation; 2. minimises the amount of data held about individuals; 3. empowers individuals to retain control of information about themselves at all times.").

[175] *See generally* Christopher Soghoian, *supra* note 48 (arguing and documenting how "telecommunications carriers and service provides play an essential role facilitating modern [law enforcement] surveillance").

[176] *See* discussion *infra* Part III.A & B.

the identities of dissidents as they seek to communicate over the Internet invisible to the threatening gaze of repressive governments.[177] This same anonymity, however, might enable criminals to shield their identities as they browse, communicate, and otherwise conduct illicit activities using communications networks.[178] The dynamic "give and take" fostered by the complex dualistic properties of such technologies is creating a similar dialogical pattern in the larger congressional public policy debate over the relative wisdom of expanding the Government's wiretapping capabilities in the face of growing and justified concerns about the cybersecurity vulnerabilities such expanded capabilities inevitably create when they are introduced into communications networks.[179]

To be clear about the limits of the inquiry here, this Article does not suggest that these specific privacy-enhancing technologies will constrain government power (i.e., limit government access to data or thwart government interception capabilities) with respect to the specific location tracking tools at issue in the *Jones* case. Rather, these technologies play a role in limiting government power in the context of the larger discussion about overly broad government access to data and its most insidious potential political effects, as described in Justice Sotomayor's concurrence.[180] On that basis, this Part will argue that, insofar as these technologies may require the Government to work harder to get information by spending more time and resources on investigating cases, they will reintroduce an element of needed fundamental friction into a law enforcement access regime in which, for decades now, the Government's gaze has been inexorably sharpened by previous technological advances.[181]

This Part takes the form of two case studies, both exploring the impact that specific privacy enhancing technologies can have: Tor,

---

[177] *See* discussion *infra* Part III.A.
[178] *See id.*
[179] *See* discussion *infra* Part III.C.
[180] *See* discussion *supra* Part II.C.
[181] *See supra* accompanying text in notes 39, 48.

an anonymization technology, and Silent Circle,[182] an encryption technology. This Part begins by explaining what each does, including the particular "give and take" dynamic promoted by the specific properties of each technology, and how each can thwart certain aspects of law enforcement investigations. This Part continues by placing these technologies and their complex dualistic properties within the dialogue of the larger public policy debate currently playing out in Congress. Finally, this Part discusses how these technologies, though they may not carry the legal clarity or authority of either a congressional or court ordered privacy mandate, may nevertheless, in the absence of direct intervention by a court or legislature, provide a kind of temporary "fix" that adjusts the prevailing imbalance of power in the Government's favor until judicial or legislative action can provide a more definitive answer.

A. *Tor*

Tor "is a network of virtual tunnels that allows people to improve their privacy and security."[183] Originally developed by the Naval Research Lab[184] and subsequently funded by the Defense Advanced Research Projects Agency ("DARPA") to facilitate anonymous online activities by government personnel,[185] Tor is an "onion routing"[186] technology which hides a user's IP address,[187]

---

[182] In the interest of full disclosure, the author was a paid consultant for Silent Circle in 2012.

[183] *Tor: Overview*, TOR, https://www.torproject.org/about/overview.html.en (last visited Feb. 21, 2013).

[184] *Id.*

[185] ANDY GREENBERG, THIS MACHINE KILLS SECRETS 139 (Dutton Inc. 2012).

[186] Onion Routing "routes a user's Internet data between a series of random volunteer 'node' computers. This process makes it virtually impossible to trace the data request back to the original user." Geoffrey A. Fowler, *Tor: An Anonymous, And Controversial, Way to Web-Surf*, WALL ST. J. (Dec. 17, 2012), http://online.wsj.com/article/SB10001424127887324677204578185382377144280.html?mod=e2tw. It "is a flexible communications infrastructure that is resistant to both eavesdropping and traffic analysis." *Id.* It is a communications intelligence technique that can identify, among other things, the sender, the receiver, and the time and length of communications messages. *See* GEORGE DANEZIS, INTRODUCING TRAFFIC ANALYSIS: ATTACKS, DEFENSES AND PUBLIC POLICY ISSUES (INVITED TALK) 3 (2005), *available at*

making it appear to originate from a Tor server rather than the actual address from which the user is connecting to the Internet. As security researcher Dr. Christopher Soghoian explains:

> When someone browses the web using Tor or a VPN service [a weaker type of anonymization technology than Tor] their Internet traffic appears to originate at the Tor or VPN server, rather than from their home connection. Thus, a US citizen located in Chicago who uses a Tor exit server in France will, to Google or Facebook, appear to be a user in France. Likewise, someone in Iran connecting to the web via a Tor exit server located in San Francisco will appear to the New York Times as a web surfer from San Francisco.[188]

Available to the public as a free service, Tor offers anonymity to its users by shielding information about a user's online activities, which can include "hiding" both the metadata (where a user is coming from and where they are going to) as well as the contents

---

http://research.microsoft.com/en-us/um/people/gdane/talks/TAIntro-prez.pdf; *Executive Summary*, ONION ROUTING, http://www.onion-router.net/Summary.html (last visited Feb. 21, 2013) ("Onion routing accomplishes this goal by separating identification from routing. Connections are always anonymous, although communication need not be. Communication may be made anonymous by removing identifying information from the data stream.").

[187] *See* GREENBERG, *supra* note 185, at 136. "IP Addresses identify the network that serves as the focal point from which a network-enabled device (a computer, tablet or smartphone) accesses the Internet. When a portable device moves from an Internet connection on one network (the network connection from one's home, for example) to an Internet connection on another network (a local coffee shop), the IP Address associated with the portable device will change." Brief of Amici Curiae in Support of Objections of Real Parties in Interest Jacob Appelbaum, Birgitta Jonsdottir and Rop Gonggrijp to March 11, 2011 Order Denying Motion to Vacate at 4, In re Application of the United States of America for an Order Pursuant to 18 U.S.C. § 2703(d), No. 1:11-dm-00003-TCB-LO (E.D. Va. Mar. 31, 2011), *available at* http://www.wired.com/images_blogs/threatlevel/2011/03/Bellovin-Amicus-in-Twitter-WikiLeaks-Case.pdf.

[188] Christopher Soghoian, *Does Using Certain Privacy Tools Expose You to Warrantless NSA Surveillance? ACLU Files FOIA to Find Out*, AM. CIVIL LIBERTIES UNION (Nov. 27, 2012, 1:04 PM), http://www.aclu.org/blog/national-security-technology-and-liberty/does-using-certain-privacy-tools-expose-you.

of communications.[189] Such anonymity prevents anyone else capable of intercepting network traffic (e.g., ISPs or government agencies) from being able to determine, for example, *who* is visiting a website or the identities of users communicating with each other.[190] If a target cannot be located on the network, it becomes difficult to intercept a target's communications. Tor also allows users to "publish websites and other services without needing to reveal the location of the site."[191] The Tor website explains:

> Using Tor protects you against a common form of Internet surveillance known as "traffic analysis." Traffic analysis can be used to infer who is talking to whom over a public network. Knowing the source and destination of your Internet traffic allows others to track your behavior and interests. This can impact your checkbook if, for example, an e-commerce site uses price discrimination based on your country or institution of origin. It can even threaten your job and physical safety by revealing who and where you are. For example, if you're travelling abroad and you connect to your employer's computers to check or send mail, you can inadvertently reveal your national origin and professional affiliation to anyone observing the network, even if the connection is encrypted.[192]

Such anonymity facilitates a variety of interests and goals pursued by various U.S. agencies. Indeed, the State Department funds Tor in order to facilitate secure communications among political

---

[189] *See TOR: Overview, supra* note 183 ("To create a private network pathway with Tor, the user's software or client incrementally builds a circuit of encrypted connections through relays on the network. The circuit is extended one hop at a time, and each relay along the way knows only which relay gave it data and which relay it is giving data to. No individual relay ever knows the complete path that a data packet has taken. The client negotiates a separate set of encryption keys for each hop along the circuit to ensure that each hop can't trace these connections as they pass through.").

[190] *See Tor Project: Anonymnity Online*, TOR, https://www.torproject.org/index.html.en (last visited Apr. 27, 2013) (explaining that "Tor protects you by bouncing your communications around a distributed network of relays run by volunteers all around the world: It prevents somebody watching your Internet connection from learning what sites you visit, and it prevents the sites you visit from learning your physical location").

[191] *Tor: Overview, supra* note 183.

[192] *Id.*

dissidents (i.e., free from surveillance by oppressive governments), and the military uses Tor for "open-source intelligence, gleaning foreign policy or military strategy from other countries' websites without tipping them off to a 'spook's' presence."[193] Moreover, "Military personnel need to use electronic resources run and monitored by insurgents. They do not want the webserver logs on an insurgent website to record a military address, thereby revealing the surveillance."[194] Similarly, law enforcement agencies use Tor for certain investigative activities (officials can visit questionable websites without alerting those running the websites to law enforcement's presence which, in most circumstances, would expose any ongoing investigation of the website) and stings or online undercover operations (regardless of how well developed and executed an undercover officer's cover may be, if his "communications include IP ranges from police addresses, the cover is blown").[195]

Use of Tor's free software has reportedly doubled in the past year, with six hundred thousand people using it every day.[196] Andrew Lewman, Tor's executive director, explains that "[t]en years ago, no one had this concept of privacy, . . . [b]ut with the [General David] Petraeus scandal and cellphones recording your location, now this doesn't seem so far-fetched anymore."[197] Indeed, fourteen percent of Tor's traffic now connects from locations in the United States and "people living in Internet-censoring countries are now Tor's second-largest user base."[198]

---

[193] GREENBERG, *supra* note 185, at 140.

[194] *Users of Tor*, TOR, https://www.torproject.org/about/torusers.html.en (last visited Feb. 21, 2013).

[195] *Id.*

[196] Fowler, *supra* note 186.

[197] *Id.* For an analysis of how a privacy-enhancing technology like Tor may have thwarted law enforcement's ability to identify Paula Broadwell, which eventually led to the discovery of her relationship with General and former CIA Director David Petraeus, see Christopher Soghoian, *Surveillance and Security Lessons From the Petraeus Scandal*, AM. CIVIL LIBERTIES UNION (Nov. 13, 2012, 4:24 PM), http://www.aclu.org/blog/technology-and-liberty-national-security/surveillance-and-security-lessons-petraeus-scandal.

[198] *Id.*

Criminals, however, can use Tor, as well. Andy Greenberg, a technology reporter for Forbes Magazine and author of a recent book about the history of the "cypherpunk" movement which aims to free the world's information concludes that "[i]t's no secret Tor is used by child pornographers and black hat hackers."[199] John Shehan, the Director of the National Center for Missing & Exploited Children, describes Tor as " 'a challenge for law enforcement,' " indicating, "[i]t is being used regularly to trade sexually exploitative images of children—although there is little Tor's creators can do about it."[200] When criminals use Tor to mask their IP addresses, which otherwise could often be "mapped to a city or even a street location"[201] by obtaining records from the target's internet service provider ("ISP"), law enforcement's efforts to identify who may have sent a threatening email or downloaded a child pornography image can be thwarted. This is because the IP address logged by the email provider or child pornography serving website will appear to be the address of one of the Tor servers, rather than an address provided to the user by their ISP.[202] Tor servers, which are comprised of volunteers around the world lending their computers to the Tor network,[203] do not keep logs and thus cannot provide any information to law enforcement about the activities of the users of the network. Law enforcement can, of course, use other, more traditional investigative techniques or different technical tools, which may include investigating opportunity and motive, finding witnesses, conducting an undercover sting operation, or technical analysis of content. But each case is different, and there is no guarantee that use of any particular technique or combination of techniques will

---

[199] GREENBERG, *supra* note 185, at 140.

[200] Fowler, *supra* note 186.

[201] *Users of Tor*, *supra* note 194.

[202] When someone browses the web using Tor, their Internet traffic appears to originate at the Tor server, rather than from their actual Internet connection, thus masking the true IP address (identity) of the individual who downloaded the child pornography image or sent the threatening email. *See supra* text accompanying note 188.

[203] The Tor network "depends on volunteers . . . whose computers help reroute and conceal Internet traffic." Fowler, *supra* note 186.

ultimately identify the suspect behind the masked IP address. Moreover, the use of such techniques merely to identify a target or several targets can be far more time consuming and resource intensive than merely sending a subpoena to an ISP.[204]

For Tor to work for the "good guys," however, the good guys cannot be the only ones who use Tor.[205] Indeed, the variety of people who use Tor is an essential part of its security protocol.[206] Tor hides an individual among a diverse group of other users on the network.[207] "Anonymity loves company":[208] The more "populous and diverse the user base," the more each user's anonymity will be protected.[209] If only law enforcement, military or human rights workers use Tor, then their identities will not be anonymous or secure because the mere connection to a Tor server would reveal their affiliation. While Tor provides security that can facilitate certain government objectives, it can, simultaneously, challenge other law enforcement missions. Indeed, Tor is a technology at the nexus of privacy and security, with a

---

[204] *See* 18 U.S.C. § 2703(c)(2) (2006) (permitting the disclosure of basic subscriber, session, and billing information with the use of "an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury subpoena"). This basic subscriber, session, and billing information includes "records of session times and durations as well as IP addresses assigned to the user during Internet connection." U.S. DEP'T OF JUSTICE, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS 138 (3d ed. 2009) [hereinafter DOJ MANUAL], *available at* http://www.justice.gov/criminal/cybercrime/docs/ssmanual2009.pdf.

[205] *See* Roger Dingledine & Nick Mathewson, *Anonymity Loves Company: Usability and the Network Effect, Proceedings of the Fifth Workshop on the Economics of Information Security*, THE FREE HAVEN PROJECT 3 (2006) *available at* http://freehaven.net/anonbib/cache/usability:weis2006.pdf ("Anonymity networks work by hiding users among users. . . . No organization can build this infrastructure for its own sole use. If a single corporation or government agency were to build a private network to protect its operations, any connections entering or leaving that network would be obviously linkable to the controlling organization. The members and operations of that agency would be easier, not harder, to distinguish.").

[206] *See id.*

[207] *Tor: Overview*, *supra* note 183.

[208] Dingledine & Mathewson, *supra* note 205, at 3.

[209] *Id.*

technological "nature" that is complex and dualistic—it gives and it takes away, sometimes forcing difficult tradeoffs among valued equities as it goes.

B. *Silent Circle*

Silent Circle is an "end-to-end"[210] encryption service offering, among other things, encrypted texts and phone calls.[211] The service can be purchased by any individual and used on his or her mobile device via the Silent Circle app.[212] The encryption keys used to protect communications are generated on the device and then erased when they are no longer needed for functionality—so they disappear when the communication is completed.[213] The Silent Circle service does not generate the encryption keys and does not hold the keys on their servers.[214] The company, therefore, has no ability to decrypt user communications.[215] Because Silent Circle does not possess the encryption keys, the company cannot provide access to anyone else, good or bad.[216] As Silent Circle explains on its website, "Our encryption keeps unauthorized people from understanding your transmissions. It keeps criminals, governments, business rivals, neighbors and identity thieves from stealing your data and from destroying your personal or corporate

---

[210] End-to-end encryption can be generally described as "a method to secure data while in flight from one device to another . . . [and] loosely define[d] as a method to protect data in flight over a network such that only each end of the transaction has the ability to see the plaintext." BRANDEN WILLIAMS, WILL END TO END ENCRYPTION SAVE US ALL? 3 (2010) *available at* https://www.brandenwilliams.com/brwpubs/WillEndtoEndEncryptionSaveUsAll.pdf.

[211] *See Silent Network – We Designed It, We Custom-Built It, & We Own The Network*, SILENT CIRCLE, https://silentcircle.com/web/silent-network/ (last visited Feb. 22, 2013).

[212] *See id.*

[213] *See id.*

[214] *See id.*

[215] *What We Do & Don't Do*, SILENT CIRCLE, https://silentcircle.com/web/what-we-do-dont-do/ (last visited Feb. 22, 2013) ("We do not have the ability to decrypt your communications across our network and nor will anyone else - ever.").

[216] *Id.*

privacy. There are no back doors in our systems, nor will there ever be."[217]

A "back door" is the general term describing a mechanism or access point in a communications device or network that enables "the creator of software or hardware [to] access data without the permission or knowledge of the user."[218] Building in such back door access, however, inevitably produces security vulnerabilities. Indeed, as security researcher Dr. Susan Landau explains:

> Building wiretapping [capabilities] into communications infrastructure creates serious risk that the communications system will be subverted either by trusted insiders or skilled outsiders, including foreign governments, hackers, identity thieves and perpetrators of economic espionage.[219]

Back doors create additional "attack surfaces,"[220] that is, code must be written to create the back door and the code must have unfettered access to communications content. The additional code creates the potential for more bugs (more code, more bugs)[221] that could be exploited to allow improper access to the system. Moreover, for a back door in an encrypted communications service

---

[217] *Id.*

[218] Peter Swire & Kenesa Ahmad, *Encryption and Globalization*, 13 COLUM. SCI. & TECH. L. REV. 416, 460 (2012).

[219] *Going Dark: Lawful Electronic Surveillance in the Face of New Technologies: Hearing Before the Subcomm. on Crime, Terrorism and Homeland Security of the H. Comm. on the Judiciary*, 112th Cong. 2 (2011) [hereinafter *Going Dark Hearing*] (statement of Dr. Susan Landau, Fellow, Radcliffe Institute for Advanced Study, Harvard University [hereinafter Landau Statement]) at 2, *available at* http://judiciary.house.gov/hearings/pdf/Landau02172011.pdf).

[220] Jim Pravetz, What's An Attack Surface?, THE ZERO TOUCH BLOG (Feb. 23, 2013), http://www.armor5.com/blog/2013/what-is-attack-surface/. ("In the world of computer security, the term *attack surface* refers to the depth of methods a hacker can use to exploit your system.")

[221] *See* Chad Perrin, *The Danger of Complexity: More Code, More Bugs*, IT SECURITY BLOG (Feb. 2, 2010), http://www.techrepublic.com/blog/security/the-danger-of-complexity-more-code-more-bugs/3076 ("If you want to produce secure software, you should focus on following the advice . . . . All else being equal, if you can find a way to eliminate lines of code without compromising the proper functioning of the software, you will probably improve the security of the software substantially.").

to offer interception functionality, the service provider must have momentary access to the unencrypted communications data.[222] As a result, if and when security flaws in the system are discovered and exploited, the worst-case scenario will be unauthorized access to users' communications. This means that when compromised, an encrypted communications system with a lawful interception back door is far more likely to result in the catastrophic loss of communications confidentiality than a system that never has access to the unencrypted communications of its users.[223]

With respect to encrypted communications systems, there are a wide range of actors who may seek to infiltrate systems and discover backdoors, including academic security researchers and "white hat" hackers who look for security vulnerabilities in

---

[222] *See Storing Passwords, or The Risk of a No-Salt Diet*, TECH@FTC (Mar. 21, 2013), http://techatftc.wordpress.com/2013/03/21/storing-passwords-or-the-risk-of-a-no-salt-diet/. When discussing best practices for storing and protect passwords, security researcher Dr. Steven Bellovin begins with a fundamental security principle: "It's a prime rule of security: something that doesn't exist can't be stolen. Conversely, if something does exist, it can be stolen or leaked in many, many ways." *Id.* This principle is applicable to law enforcement-enabled back doors as well: If they exist, they will be discovered and exploited.

[223] *See generally* Vassilis Prevelakis and Diomidis Spinellis, *The Athens Affair: How Some Extremely Smart Hackers Pulled Off the Most Audacious Cell-Network Break-In Ever*, IEEE SPECTRUM (June 29, 2007, 18:33 GMT), http://spectrum.ieee.org/telecom/security/the-athens-affair (describing how "hackers broke into a [Greek] telephone network and subverted its built-in wiretapping features for their own purposes . . . . While the hack was complex, the taps themselves were straightforward. When the [Greek] prime minister, for example, initiated or received a call on his cellphone, the exchange would establish the same kind of connection used in a lawful wiretap—a connection to a shadow number allowing it to listen in on the conversation"); *see generally* U.S. NAT'L SEC. ASS'N, PHONE FREAKS CAN INVADE YOUR PRIVACY (1976), *available at* http://explodingthephone.com/docs/db904 (describing how interfaces used by phone company employees to determine if a line was busy were subverted by outsiders to listen to phone conversations).

The author is indebted to Dr. Christopher Soghoian for several discussions in which he explained the various reasons why introducing back doors into encrypted systems inevitably renders those systems less secure (interview with Dr. Christopher Soghoian on Mar. 14, 2013 and Apr. 6, 2013, and to Dr. Steven Bellovin for providing additional source material illustrating that conclusion.

systems and earn money by disclosing the information to the authors of the products or the public.[224] Other actors include "large organized crime operations that possess ample resources to attract costly computer security talent, or foreign governments."[225] After gaining access to or breaking into a system, an insider or intruder can subvert built-in wiretapping capabilities for his own purposes.[226] There is no way to create a back door that will work only for legitimate surveillance when an intruder breaches a system or an insider gains unauthorized access to and use of that back door.[227]

Taking steps to protect communications and data is critical at a time when "cyberexploitations have become constant occurrences," and many U.S. companies and government sites have been targeted.[228] According to Dr. Landau:

> The modus operandi is always the same. Some software vulnerability—unpatched software, a user opening a targeted mail that contains malware (or that directs the user to a site with malware—allows the intruder in. The intruder spend[s] time carefully studying the site and finding the files of interest. At some point, the intruder efficiently ships out copies. This is carefully done. By the time the corporate or government site becomes aware that there has been an intrusion, it is often too late. The data has been shipped to China. Organizations that have been exploited in this way cut across large swaths of American industry and government, including such leading members as Google, Lockheed Martin, NASA, Northrup Grumman, Oak Ridge [and] National Laboratory.[229]

Silent Circle's products offer users—whether they are individuals, corporations or government clients—an important defense against

---

[224] Swire & Ahmad, *supra* note 218, at 460.

[225] *Id.*

[226] *See* Prevelakis & Spinellis, *supra* note 223.

[227] *See id.*; *see also* Swire & Ahmad, *supra* note 218, at 433 ("The main problem with backdoors, however, is that it is extremely difficult to install a backdoor that can be used by the 'good guys,' such as authorized law enforcement wire tappers, but not by the 'bad guys.' ") (citing SUSAN LANDAU, SURVEILLANCE OR SECURITY? THE RISKS POSED BY NEW WIRETAPPING TECHNOLOGIES 175–202 (MIT Press 2011)).

[228] Landau Statement, *supra* note 219, at 2.

[229] *Id.* at 4.

cyberexploitations because encryption keys are held by the users on their mobile devices, then erased when no longer needed, thus making it impossible for Silent Circle to give keys, willingly or unwillingly, to anyone else.[230] Moreover, the Silent Circle system has no back doors. Accordingly, any compromise of the Silent Circle servers would only permit the interception of encrypted communications that, without the encryption keys stored only on users' devices, would be an indecipherable cloud of ones and zeros.[231]

As descriptors like "end-to-end" encryption and claims to have "no back doors in our systems" point to a high security threshold, they also suggest to users that even lawfully authorized surveillance by "good" governments will be challenging, if not impossible. Indeed, just as adversaries will encounter an indecipherable cloud of computer code, lawfully authorized intercepts would have no clearer view.[232] Silent Circle and similar products will, therefore, force governments to find other ways to acquire target communications at a point in time when they are not encrypted. Such options, which may not be possible in all cases, are time and resource intensive, do not scale, and cannot be used to conduct nationwide surveillance.[233]

At this point in the discussion, however, it is worth noting the dualistic "give and take" properties of end-to-end, user-held key encryption products like Silent Circle for voice and text communications. As discussed, they are an important defense in the age of cyberexplotations. However, they may also thwart the Government's ability to intercept communications in a timely fashion, causing the Government to lose valuable evidence or preventing the government from acquiring a target's communications completely. [234] Indeed, Silent Circle is a

---

[230] *See* SILENT CIRCLE, *supra* note 215.

[231] *See id.*

[232] *See id.*

[233] *See infra* Part III.C.

[234] Many of the observations about law enforcement investigations in this Article are drawn from the author's experience as a former federal prosecutor and a former counsel to the House Judiciary Committee.

technology at the cusp of a public policy debate where stronger cybersecurity practices (which in turn bolster U.S. national security) may force tradeoffs with surveillance capabilities that enable traditional law enforcement efforts.[235]

C. *The Larger Public Policy Debate*

In the fall of 2010, at least one news outlet reported that the FBI was preparing to seek an expansion[236] of a 1994 law called the Communications Assistance for Law Enforcement Act ("CALEA").[237] CALEA was enacted "to ensure law enforcement surveillance capabilities remained intact during the move from a copper-wire phone systems to digital networks."[238] With this technological shift, CALEA required "telephone companies, telecommunication service providers, and manufacturers of telecommunication equipment ... to update their equipment, facilities, and services to ensure built-in surveillance capabilities" that would allow law enforcement agencies to monitor and access communications in real-time.[239] CALEA even required telephone companies to provide and allow the FBI to review new technologies prior to their implementation.[240] The exponential growth of the Internet was just beginning when CALEA was

---

[235] *See infra* Part III.C. In addition, for government personnel who may use Silent Circle to facilitate secure communications in operational situations where it is also important that they maintain a non-government cover, the diversity of the Silent Circle user base facilitates the cover. If only government personnel used Silent Circle (and had the Silent Circle app on their mobile device), then their government identities could not remain secret. Like Tor then, for Silent Circle to work for certain types of government personnel and missions, it must be available to the general public. *See supra* Part III.A.

[236] *See* Charlie Savage, *U.S. Tries to Make It Easier to Wiretap the Internet*, N.Y. TIMES (Sept. 27, 2010), http://www.nytimes.com/2010/09/27/us/27wiretap.html?_r=0 ("Federal law enforcement and national security officials are preparing to seek sweeping new regulations for the Internet, arguing that their ability to wiretap criminal and terrorism suspects is 'going dark' as people increasingly communicate online instead of by telephone.").

[237] 47 U.S.C. §§ 1001–1010 (2006).

[238] Swire & Ahmad, *supra* note 218, at 421.

[239] *Id.*

[240] *Id.* at 422.

enacted and, as Professor Peter Swire and Kenesa Ahmad assert, "The legislative compromise at the core of CALEA provided that new wiretap ready requirements only applied to voice networks and *did not apply to internet protocol communications*."[241]

The proliferation of new Internet hardware and software technologies continued apace as Internet usage grew exponentially, exceeding four hundred million people in the year 2000, so it is not hard to imagine how a requirement that the FBI review each new CALEA-compliant technology before its deployment might have hampered, perhaps even crippled, such innovation.[242] The resulting effects of non-CALEA covered communication technologies on wiretapping capabilities, however, have not been friendly to law enforcement. In a 2011 House Judiciary Committee hearing entitled "Going Dark: Lawful Electronic Surveillance in the Face of New Technologies," former FBI General Counsel Valarie Caproni testified as follows:

> In the ever-changing world of modern communications technologies . . . the FBI and other government agencies are facing a potentially widening gap between our legal *authority* to intercept electronic communications pursuant to court order and our practical *ability* to actually intercept those communications. . . . We call this capabilities gap the "Going Dark" problem. As the gap between authority and capability widens, the government is increasingly unable to collect valuable evidence in cases ranging from child exploitation and pornography to organized crime and drug trafficking to terrorism and espionage—evidence that a court has authorized the government to collect. This gap poses a growing threat to public safety. . . . [D]ue to the revolutionary expansion of communications technology in recent years, the government finds that it is rapidly losing ground in its ability to execute court orders with respect to Internet-based communications that are not covered by CALEA.[243]

---

[241] *Id.* at 422 (emphasis added) (citing 47 U.S.C. § 1002(b)(2)(A) (2006)) (excluding "information services").

[242] *See id*; *see also* LANDAU, *supra* note 227, at 189 ("Applying CALEA-compliance requirements to any application with communications would have extremely negative impacts on innovation and the U.S. economy.").

[243] *Going Dark Hearing*, *supra* note 219 (statement of Valerie Caproni, General Counsel, Federal Bureau of Investigation) [hereinafter Caproni

It is important to recognize that the FBI General Counsel has described a problem with wiretapping capabilities, not a lack of the legal authority to conduct surveillance. Moreover, her use of the phrase "gap between authority and capability" can be interpreted to refer not only to new Internet-based technologies not covered under CALEA's wiretapping requirements, but also to other technological barriers, like encryption, which create a gap between the authority to intercept communications and the capability to execute the surveillance.[244] Indeed, there was a time in history when law enforcement actively opposed encryption technologies that did not contain government-mandated back doors. In 1997, Former FBI Director Louis Freeh testified to the House Committee on International Relations that law enforcement:

> [I]s [seeking] a balanced encryption policy, one that will allow the technology to progress, but at the same time put in there a safety valve and an access point controlled by the courts which myself and people in the Intelligence Community can get to and understand evidence where it is important for us to do so. . . . The inability to deal with robust encryption, the lack [of] any access in real-time, to this information in . . . many cases, will, in my view . . . affect public safety and maybe even tragically cost lives.[245]

In that same year, the House Intelligence Committee passed a bill out of Committee, "drafted in large part by the FBI," imposing "criminal penalties . . . [for] manufacturing or distribut[ing] domestic encryption products that did not contain a government-mandated back door."[246] In an Article examining the debate on

---

Statement], at 1, *available at* http://judiciary.house.gov/hearings/pdf/Caproni02172011.pdf).

[244] Swire & Ahmad, *supra* note 218, at 464 n.141; *see also* Max Eddy, *The Real Reason the Feds Can't Read Your iMessages*, SECURITY WATCH (Apr. 4, 2013, 12:29 pm), http://securitywatch.pcmag.com/none/310015-the-real-reason-the-feds-can-t-read-your-imessages (describing how encryption and the lack of CALEA-mandated wiretapping capabilities thwart law enforcement's ability to intercept real-time messages sent over Apple's iMessage system).

[245] *Member Briefing Regarding Encryption: Hearing Before the H. Comm. On International Relations*, 105th Cong. 6–8 (1997) (statement of Louis J. Freeh, Director, Federal Bureau of Investigation), *available at* http://cryptome.org/jya/hir-hear.htm.

[246] Swire & Ahmad, *supra* note 218, at 438.

encryption policies in the face of increasing globalization, Professor Swire and Kenesa Ahmad document the factual, policy and legal arguments informing the three stages of the so-called "crypto wars" of the 1990s, with the third and final stage representing the Clinton Administration's position shift in 1999 that lifted most export controls on encryption.[247] This action signaled that the Government had "explicitly endorsed the view that strong encryption is needed for the Internet."[248] Their scholarship illustrates, however, that the legality of the type of encryption service offered by Silent Circle—one in which there are no government back doors—has not always been a foregone conclusion.[249] Professor Swire, who was chair of the White House Working Group on Encryption preparing for the 1999 announcement, explains that, over time, it became clear that "no technical fix . . . was available to provide access only to the 'good guys' but not the 'bad guys.' "[250]

With the looming possibility of an Obama Administration proposal to expand CALEA,[251] security researchers Dr. Steven Bellovin, Dr. Matt Blaze, Sandy Clark and Dr. Susan Landau recently proposed options to address the growing gap between law

---

[247] *See id.* at 439.

[248] *Id.* at 440.

[249] *See id.* at 437–41.

[250] *Id.* at 440–41. Hacking software is no longer a secretive government tool. *See, e.g.*, *Servers in Canada Linked to FinFisher Spyware Program*, CBC NEWS, (Mar. 13, 2013), http://www.cbc.ca/news/politics/story/2013/03/13/pol-cp-cybersecurity-germany-spyware-canada.html ("Researchers said Wednesday that they have identified 25 countries that host servers linked to FinFisher, a Trojan horse program which can dodge anti-virus protections to steal data, log keystrokes, eavesdrop on Skype calls, and turn microphones and webcams into live surveillance devices.").

[251] *See* Declan McCullagh, *FBI: We Need Wiretap-Ready Web Sites—Now*, CNET (May 4, 2012, 9:24 AM), http://news.cnet.com/8301-1009_3-57428067-83/fbi-we-need-wiretap-ready-web-sites-now/ (claiming that "[t]he FBI is asking Internet companies not to oppose a controversial proposal that would require firms, including Microsoft, Facebook, Yahoo, and Google, to build in backdoors for government surveillance").

enforcement surveillance authorities and capabilities.[252] Their primary and provocative solution is to enable and expand FBI hacking capabilities rather than give them back doors.[253] In other words, these researchers assert that "a better way to protect privacy and security on the internet may be for the FBI *to get better at breaking into computers*."[254] Rather than requiring the insertion of back doors—whether by way of a CALEA-type mandate where wiretapping capabilities are built into the architecture of communications networks, devices and applications, or through hidden "lawful intercept" access features[255]—law enforcement should "exploi[t] naturally occurring weaknesses in subjects' devices, enabling law enforcement to install surreptitious interception software at a target endpoint as required."[256] This option represents a fundamental paradigm shift away from mandated communications network-based interception (i.e., CALEA mandated wiretapping capabilities built into carrier networks), to a focus on exploiting specific "software vulnerabilities [that] exist whether or not law enforcement uses them against its targets."[257] Moreover, while maintaining some law enforcement wiretapping capabilities, this option avoids the security vulnerabilities, risks and costs associated with nationally mandated wiretap interfaces.[258]

With respect to encrypted communications, this kind of successful device exploitation would allow law enforcement to acquire content communications before they are encrypted or after they are decrypted—even when using an encryption service like

---

[252] *See* Steven M. Bellovin, Matt Blaze, Sandy Clark & Susan Landau, *Going Bright: Wiretapping without Weakening Communications Infrastructure*, 14 IEEE SECURITY & PRIVACY 62, 62 (2013).

[253] *See* Matt Blaze & Susan Landau, *The FBI Needs Hackers, Not Backdoors*, WIRED (Jan. 14, 2013, 8:00 AM), http://www.wired.com/opinion/2013/01/wiretap-backdoors/.

[254] *Id.* (emphasis added).

[255] *See* Bellovin, Blaze, Clark & Landau, *supra* note 252, at 63.

[256] *Id.* at 62–63.

[257] *Id.* at 71.

[258] *Id.* at 63.

Silent Circle.[259] To support the viability of this "hacker" option, these security researchers explain how law enforcement might go about developing tools that exploit target endpoint vulnerabilities and, in turn, maintain such exploitation capabilities.[260] It is important to recognize, however, that these device-centered exploitation capabilities will not scale anywhere near as easily or in as expansive a manner as CALEA's nationally mandated wiretap interfaces do.[261] Law enforcement's overall wiretapping

---

[259] *See* SILENT CIRCLE, *supra* note 215. Ultimately, the Silent Circle service "can't protect you against malware, spyware, or bugs in the OS [(operating system)] or [] software." *Id.* In other words, if malware or spyware has been installed by law enforcement or other entities on a target mobile device, law enforcement may be able to acquire the communications in an unencrypted format, notwithstanding the individual's use of Silent Circle or other encryption services. *Id.*

[260] *See* Bellovin, Blaze, Clark & Landau, *supra* note 252, at 66–68. These researchers also briefly discuss (but do not fully address in their current Article) that this hacker option raises a number of its own policy considerations including the complex questions involved in making law enforcement an active participate in the "vulnerabilities market." *Id.* at 69. For example, "Law enforcement demand [for software vulnerabilities] might help skew incentives against disclosing patches to the software vendors themselves, and some have argued that the process increases the amount of software left unpatched." *Id.* (internal citations omitted). It is also beyond the scope of this Article to discuss and evaluate the policy implications of turning the FBI into hackers for purposes of facilitating law enforcement wiretapping capabilities.

[261] This is because, rather than relying on a CALEA-type centralized, nationally mandated system for wiretapping capabilities, law enforcement's ability to intercept target communications will rely on whether or not vulnerabilities have been discovered on the specific mobile device used by the target. *See* Bellovin, Blaze, Clark & Landau *supra* note 252, at 62 ("Continuing technical access to authorized wiretaps can be achieved—without expanding CALEA—by exploiting naturally occurring weaknesses in subjects' devices, enabling law enforcement to install surreptitious interception software at a target endpoint as required."). Moreover, each time law enforcement agencies exploit the vulnerability, they risk the discovery of the flaw by security researchers. After the vulnerability is discovered and reported to the software vendor, it will be patched and can no longer facilitate law enforcement exploitation against targets running the latest software, forcing law enforcement to find another wiretapping method. *See id.* at 63 ("Many such weaknesses are *0-day vulnerabilities*, ones that might be completely unknown to others and for which no vendor fix exists. (Conceptually, the bug is discovered on day zero and

efforts will, therefore, become more time and labor intensive and perhaps relatively less effective in acquiring evidence in investigations. Perhaps recognizing this reality, while also understanding the security benefits inherent in strong encryption technologies, FBI General Counsel Caproni acknowledged in her congressional testimony that:

> Addressing the Going Dark problem does not require fundamental changes in encryption technology. We understand that there are situations in which encryption will require law enforcement to develop *individualized solutions*.[262]

Such "individualized solutions," whether attempted through broad implementation of an FBI-as-"hacker" policy model or through more traditional investigative techniques, like the use of undercover agents and informants, may not be possible in every case. Indeed, Bellovin, Blaze, Clark and Landau acknowledge that "some targets will use communications systems for which penetration is very difficult or expensive under our proposed scheme." [263] Moreover, Caproni warned Congress about a surveillance environment where individualized solutions must be the rule rather than the exception:

> There will always be criminals, terrorists, and spies who use very sophisticated means of communications that are going to create very specific problems for law enforcement. We understand that there are times when you need to design an individual solution for an individual target . . . . We are looking for a better solution for most of our targets, and the reality is, I think, sometimes we want to think that criminals are a lot smarter than they really are. Criminals tend to be some-what lazy, and a lot of times, they will resort to what is easy. And, so long as we have a solution that will get us the bulk of our targets, the bulk of criminals, the bulk of terrorists, the bulk of spies, we will be ahead of the game. We can't have individual—have to design individualized solutions as though they were a very sophisticated target who was self-encrypting and putting a very difficult encryption algorithm on for

---

reported and patched sometime later.)").

[262] Caproni Statement, *supra* note 243, at 3 (emphasis added).

[263] Bellovin, Blaze, Clark & Landau, *supra* note 252, at 67.

> every target we confront because not every target is using such sophisticated communications.[264]

Ms. Caproni's testimony suggests that, while law enforcement resources may be able to accommodate the use of encryption by the relatively limited number of truly "sophisticated criminals," a more pervasive adoption of encryption by "mainstream" criminals will overtax law enforcement resources. Indeed, if growing numbers of garden variety criminals begin using encryption products with no government-enabled back doors, then law enforcement will be forced to make investigative choices, prioritizing the most serious of investigations and de-emphasizing others, if not dropping them altogether.

A surveillance environment defined by a more pervasive availability and adoption of encryption products like Silent Circle that may harm law enforcement investigative equities will force Congress to confront tradeoffs between what might be characterized as the more the traditional public safety mission of law enforcement and necessary efforts to enhance cybersecurity, a fundamental element of our greater national security. Indeed, Dr. Landau has instructed Congress:

> Beginning in this decade, the world shifted in two fundamental ways that substantively changed the nature of this type of industrial espionage; it was made cheaper, and there was a very large customer for the information. The growth of the Internet and computing technology has greatly simplified the ability of spies, especially those at a distance, to get "inside" a company. The other change is China. Well aware of the information infrastructure asymmetry between China and the U.S., China is seeking to use the asymmetry to its advantage. Other nations also exploit our heavy dependence on cyber infrastructure but China seems particularly active in doing so.[265]

The accuracy of Dr. Landau's warnings to the House Judiciary Committee about China's propensity to engage in industrial espionage efforts against the U.S. is becoming increasingly more

---

[264] *Going Dark Hearing, supra* note 219, at 52 (oral testimony of Valerie Caproni, General Counsel, Federal Bureau of Investigation), *available at* http://judiciary.house.gov/hearings/printers/112th/112-59_64581.PDF.

[265] Landau Statement, *supra* note 219, at 5.

public and pervasive. Consider the recent Mandiant Report[266] documenting various exploits of some of the most sophisticated Chinese government hacking groups. "Comment Crew," for example, "has drained terabytes of data from companies like Coca-Cola [but], increasingly its focus is on companies involved in the critical infrastructure of the United States—its electrical power grid, gas lines and waterworks."[267] Moreover, "[O]ne target was a company with remote access to more than 60 percent of oil and gas pipelines in North America. The unit was also among those that attacked the computer security firm RSA, whose computer codes protect confidential corporate and government databases."[268]

In October 2012, the House Permanent Select Committee on Intelligence issued a bi-partisan report entitled, "Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE," which asserted that "China has the means, opportunity, and motive to use telecommunications companies for malicious purposes," and that "Chinese actors are ... the world's most active and persistent perpetrators of economic espionage." [269] In analyzing the significant supply chain threats products produced by these companies pose, "the Committee took seriously recent allegations of backdoors ... [and] other unexpected elements in either company's products."[270]

---

[266] Exposing One of China's Cyber Espionage Units, MANDIANT, http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf (last visited Apr. 14, 2013).

[267] David E Sanger, David Barboza & Nicole Perlroth, *Chinese Army Unit Is Seen as Tied to Hacking Against U.S.*, N.Y. TIMES (Feb. 18, 2013), http://www.nytimes.com/2013/02/19/technology/chinas-army-is-seen-as-tied-to-hacking-against-us.html.

[268] *Id.*

[269] H. PERMANENT SELECT COMM. ON INTELLIGENCE, 112th Cong., INVESTIGATIVE REP. ON THE U.S. NAT'L SEC. ISSUES POSED BY CHINESE TELECOMMS. CO. HUAWEI AND ZTE 2 (2012) (Chairman Mike Rogers and Ranking Member C.A. Dutch Ruppersberger), *available at* http://intelligence.house.gov/sites/intelligence.house.gov/files/documents/Huawei-ZTE%20Investigative%20Report%20%28FINAL%29.pdf.

[270] *Id.* at 11.

In March 2013, James R. Clapper, the Director of National Intelligence, presented a written statement to the Senate Select Committee on Intelligence containing, among other things, a descriptive cyber threat assessment.[271] Director Clapper discusses the erosion of our economic and national security:

> Foreign intelligence and security services have penetrated numerous computer networks of US Government, business, academic, and private sector entities. Most detected activity has targeted unclassified networks connected to the Internet, but foreign cyber actors are also targeting classified networks. Importantly, much of the nation's critical proprietary data are on sensitive but unclassified networks; the same is true for most of our closest allies.[272]

Director Clapper also explains how cybercriminals, aided by computer intrusion kits, are damaging US economic and national security interests:

> Cyber criminals also threaten US economic interests. They are selling tools, via a growing black market, that might enable access to critical infrastructure systems or get into the hands of state and nonstate actors. In addition, a handful of commercial companies sell computer intrusion kits on the open market. These hardware and software packages can give governments and cybercriminals the capability to steal, manipulate, or delete information on targeted systems. Even more companies develop and sell professional-quality technologies to support cyber operations—often branding these tools as lawful-intercept or defensive security research products. Foreign governments already use some of these tools to target US systems.[273]

With the growing awareness of such multi-faceted cyber threats, recommendations for the general use of encryption for communications and cloud data storage are coming from a range of sources. In March 2010, Federal Trade Commissioner Pamela Jones Harbour called on cloud computing providers to enable Hypertext Transfer Protocol Secure ("HTTPS") encryption[274] by

---

[271] *Worldwide Threat Assessment of the US Intelligence Community: Statement for the Record for the S. Select Comm. On Intelligence*, 113th Cong. (2013) (statement of James R. Clapper, Director of National Intelligence), *available at* http://intelligence.senate.gov/130312/clapper.pdf.

[272] *Id.* at 6.

[273] *Id.* at 7.

[274] Christopher Soghoian, *Caught in the Cloud: Privacy, Encryption, and Government Back Doors in the Web 2.0 ERA*, 8 J. TELECOMM. & HIGH TECH L.

default.[275] Following the release of a plugin for the Firefox browser called Firesheep that made it easy for a an average person to "hijack" non-HTTPS browsing sessions, Senator Chuck Schumer called on several major cloud computing companies to enable HTTPS by default.[276] Richard Falkenrath and Paul Rosenzweig, two former high ranking Homeland Security officials in the Bush Administration, explain that encrypting data stored in the cloud, where the customer holds the encryption keys allows the customer to "maintain exclusive control of their data," thereby avoiding certain security concerns inherent in cloud storage.[277] Indeed, if the data are encrypted locally before being transferred to the cloud, "then it just doesn't matter who works at the server farm or where the data is located (data can be stored in a number of locations both inside and outside the United States), since no one can see the data except the customer."[278]

The preceding discussion in this Part focused on the public policy debate surrounding wiretapping capabilities for purposes of obtaining real-time content communications, a debate that anticipates DOJ and the FBI seeking Congressional action. While this discussion has primarily focused on how encryption

---

359, 375 (2010) ("Bank of America, American Express and Amazon all use the industry standard Hypertext Transfer Protocol Secure (HTTPS) encryption protocol to ensure that all customer information is securely transmitted over the network. This technology enables a user to safely conduct business online, without the risk of a hacker capturing her private data as it crosses the network. This is because to third parties, her encrypted communications appear as undecipherable gibberish.").

[275] Pamela Jones Harbour, Commissioner, Fed. Trade Comm'n, Remarks Before Third Federal Trade Commission Exploring Privacy Roundtable in Washington, D.C. at 6–7 (Mar. 17, 2010), *available at* www.ftc.gov/speeches/harbour/100317privacyroundtable.pdf.

[276] Soghoian, *supra* note 48, at 50–51 (citing Lance Whitney, *Senator Wants More Secure Web Sites for Wi-Fi Use*, CNET (Feb. 29 2011, 9:10 AM), *available at* news.cnet.com/8301-1009_3-20037253-83.html.

[277] Richard Falkenrath & Paul Rosenzweig, *Op-Ed: Encryption, Not Restriction, Is the Key to Safe Cloud Computing*, NEXTGOV (Oct. 5, 2012), http://www.nextgov.com/cloud-computing/2012/10/op-ed-encryption-not-restriction-key-safe-cloud-computing/58608/.

[278] *Id.*

technologies like Silent Circle may exacerbate the FBI's "Going Dark" problem, Tor (and other anonymous browsing technologies) plays its own role in this surveillance debate, as well. From a technical standpoint, Tor frustrates wiretapping capabilities by masking a user's IP address, thereby making it difficult for law enforcement to locate a target.[279] While the FBI General Counsel's 2011 "Going Dark" congressional testimony did not call out Tor, neither federal nor state and local law enforcement has been silent about potentially losing the ability to identify a suspect and her location when she uses communication systems to commit crimes. Indeed, in 2011 when the House Judiciary Committee was considering legislation that would have required certain types of service providers[280] to maintain records reflecting users' online activities for a specific amount of time[281] so that they would be available to law enforcement if and when needed for criminal investigations,[282] state and federal law enforcement organizations

---

[279] *See supra* Part III.A. Dr. Susan Landau notes, however, that Tor and other anonymized communications systems "have high overhead and are not expected to be used by the vast majority of users." LANDAU, *supra* note 227, at 199.

[280] Tor is not a service provider and Tor network servers retain no logs that could be provided to law enforcement. *See supra* Part III.A.

[281] *See* Protecting Children From Internet Pornographers Act of 2011, H.R. 1981, 112th Cong. § 4(h)(1) (2011) (requiring a commercial provider of an electronic communication service to retain for at least one year a log of the temporarily assigned network addresses assigned to subscribers or customers that enables the identification of corresponding customer or subscriber information); *see also* Protecting Children From Internet Pornogrpahers Act of 2011, S. 1308, 112th Cong. 2011 § 4(h) (2011) (requiring a provider of an electronic communication service or remote computing service to retain for at least eighteen months a log of the temporarily assigned network addresses the service assigns to each subscriber account unless that address is transmitted by radio communication).

[282] *Data Retention as a Tool for Investigating Internet Child Pornography and Other Internet Crimes: Hearing Before the Subcomm. on Crime, Terrorism, and Homeland Security*, 112th Cong. 1 (2011) [hereinafter *Data Retention Hearing*], (opening statement of Chairman James Sensenbrenner), *available at* http://judiciary.house.gov/hearings/hear_01252011.html ("Today's hearing examines the role of data retention as a law enforcement tool to investigate the distribution of child pornography on the Internet and other online crimes. Many Internet Service Providers, ISPs currently retain data that can be used to identify

expressed their general support for mandated data retention periods.[283] A thorough discussion of the privacy and security implications of mandated data retention periods and the challenges of trying to regulate, with legislation, an open source privacy enhancing technology like Tor[284] is beyond the scope of this

---

the operator or user of an illegal Web site. But not all ISPs retain this important data, and the length of time such data is retained often varies from one provider to the next. The issue of data retention is not new. In 1999, then Deputy Attorney General Eric Holder said that certain data must be retained by ISPs for reasonable periods of time so that it can be accessible to law enforcement.").

[283] *See id.* at 11 (statement of Jason Weinstein, Deputy Assistant Attorney Gen., of the United States, Criminal Division) ("There is no doubt among public safety officials that the gaps between providers' retention policies and law enforcement agencies' needs can be extremely harmful to the agencies' investigations. In 2006, forty-nine Attorneys General wrote to Congress to express 'grave concern' about 'the problem of insufficient data retention policies by Internet Service Providers.' They wrote that child exploitation investigations 'often tragically dead-end at the door of Internet Service Providers (ISPs) that have deleted information critical to determining a suspect's name and physical location.' The International Association of Chiefs of Police adopted a formal resolution stating that 'the failure of the Internet access provider industry to retain subscriber information and source or destination information for any uniform, predictable, reasonable period has resulted in the absence of data, which has become a significant hindrance and even an obstacle in certain investigations.' In 2008 testimony before this Committee, FBI Director Robert Mueller reported that 'from the perspective of an investigator, having that backlog of records would be tremendously important,' and that where information is retained for only short periods of time, 'you may lose the information you need to be able to bring the person to justice.' Former Attorney General Gonzales similarly testified about 'investigations where the evidence is no longer available because there's no requirement to retain the data.' "); *see also id.* at 21 (statement of Chief John M. Douglass, Chair, Mid-Sized Cities Section International Association of Chiefs of Police) ("[T]here are cases where we are not able to work quickly enough—mostly because a 'lead' is discovered after the logs have expired or we are unaware of the specific service provider's protocols concerning data retention time periods.").

[284] Open-source generally refers to "a program in which the source code is available to the general public for use and/or modification from its original design free of charge." *Open Source*, WEBOPEDIA, http://www.webopedia.com/TERM/O/open_source.html (last visited Apr. 3, 2013). A foreign government's attempt to mandate a government back door in open source anonymization technology similar to Tor resulted in the discovery of the offending code, which

Article. But that is not to say that the issue of data retention has been erased from either the law enforcement or the congressional agenda.

As Congress considers options, whatever they may be, to address the "Going Dark" problem, a reckoning will occur—one in which Congress will be forced to accommodate the complex dualistic properties of technologies that, on one hand, bolster our national security against certain kinds of threats (i.e., cyberexploitations) while, on the other, they limit or thwart law enforcement's ability to fulfill its traditional public safety function by investigating crimes, notwithstanding the fact that law enforcement may have the legal authority to collect information using a particular technique. Privacy enhancing technologies like those described in this Article have the potential to frustrate the legitimate investigation of serious crimes like child pornography by law enforcement agencies, but also to protect individuals, businesses and government agencies from cyber attacks and espionage perpetrated by foreign governments. Although most policy makers would probably prefer not to have to choose between law enforcement and national security equities, the potential widespread availability and use of such technologies may make that choice an impossible one to avoid. Before Congress can regulate effectively, it will have to reckon with, and account for, "code" as both regulator and law.

D. Jones*ing For A Privacy Mandate, Getting a Technology Fix*

If we assess the Court's decision in *Jones* solely as an attempt to create a clear rule or principle that sets appropriate limits on the Government's power to track the movements of its citizens with various types of location technologies, yet enables law enforcement to use such tracking tools effectively in its investigations, the decision must be seen as a noble failure. The

---

could be re-written by security researchers and re-released for use by the public without the back door. *See* Soghoian, *supra* note 274, at 409–11 (describing the German government's attempt to mandate a back door in Java Anonymous Proxy, an open source project aimed at providing users with the ability to browse the Internet anonymously).

majority's holding is too narrow to apply to any tracking technologies that do not require the physical attachment of a GPS device on personal property.[285] To date, Congress has fared no better in its attempts to address these matters legislatively.[286] The concurring opinions in *Jones* endorse some form of a "mosaic theory" as a way to constrain the increase in government power enabled by twenty-first century location tracking technologies that do not depend upon physical trespass.[287] But the mosaic theory has the potential to wreak havoc upon the process by which courts determine whether a search has occurred and, if it has, whether it was reasonable.[288] The theory is thus unworkable for implementing Fourth Amendment protections. Justice Sotomayor's concurrence holds out the yet unfulfilled additional promise of Fourth Amendment protections that will not treat secrecy as a prerequisite for privacy—that is, a promise to reexamine the appropriateness of the third party doctrine in the digital age.[289] At best, then, the *Jones* concurrences, even if they cannot provide clear Fourth Amendment doctrine, serve to reinforce the general intuitive recognition, shared by their authors, that a new privacy mandate is needed. But the specific solutions offered in *Jones*—application of the mosaic theory and reconsideration of the third party doctrine—leave us all still *Jones*ing for an adequate answer.

There is, however, a third and different form of authority that serves to constrain government power in the digital age. That authority is technology itself, discussed here in the form of two specific types of encryption and anonymization technologies that make it more difficult, in some cases perhaps impossible, for law enforcement to obtain the information it seeks.[290] Indeed, by forcing law enforcement to use non-scalable "individualized solutions" to obtain content communications, which may include

---

[285] *See supra* Part II.A.
[286] *See supra* Part II.D.
[287] *See supra* Part II.B.
[288] *See supra* Part II.B.
[289] *See supra* Part II.C.
[290] *See supra* Part III.

acquiring a target's communications through his individual device rather than from CALEA-compliant communications carriers (like phone companies), or simply using more traditional techniques like undercover agents and sources to gather evidence in a case, encryption technologies like Silent Circle introduce a measure of friction back into the surveillance ecosystem.[291] Similarly, anonymization technologies like Tor, which mask a user's IP address, may require law enforcement to work much harder to determine the identity and location of an individual or individuals using communications systems to commit crimes—in some cases, law enforcement efforts may prove impossible.[292]

These specific privacy-enhancing technologies have dualistic "give and take" properties: on the one hand providing increasingly important security in an environment where nation state espionage and IP theft is a top national security threat and, on the other, potentially thwarting law enforcement investigations.[293] During the coming year, if Congress, as has been forecast,[294] examines new DOJ and FBI proposals for expanding the CALEA, whatever they may be, the need to protect the security of our networks will surely be a significant consideration as the legislative process proceeds.[295] As discussed, however, there is no technically feasible way to provide back doors to good guys without also making them accessible to bad guys.[296] Moreover, for anonymization technologies like Tor to work on an individual operational level for various types of government personnel, they must also be available to the general public.[297] Indeed, the diversity of the user base is an essential part of Tor's security protocols—if only government personnel use Tor, their identities will not be secure.[298]

---

[291] *See supra* Part III.
[292] *See supra* Part III.A.
[293] *See supra* Part III.C.
[294] *See supra* note 260.
[295] See *supra* Part III.C.
[296] *See supra* Part III.C.
[297] *See supra* Part III. A.
[298] *See supra* Part III. A.

Privacy-enhancing technologies like Tor and Silent Circle are, in effect, helping to advance the communications privacy dialogue insofar as they link certain aspects of electronic privacy with security. Moreover, although they do not carry the legal clarity or authority of a judicial mandate or congressional action through legislation, these privacy-enhancing technologies nevertheless offer the promise of a temporary "technology fix" that might adjust the prevailing imbalance of power in the favor of government surveillance activities until judicial or legislative action can provide a more definitive answer. To be sure, they are not a privacy mandate. At least in the short run, however, they offer a quick, sure mechanism to constrain the palpable growth of government power noted with such apprehension by some of the Justices in *Jones*.

IV. CONCLUSION

Following the D.C. Circuit's *Maynard*[299] decision—where the first manifestation of a Fourth Amendment mosaic-type theory appeared[300]—DOJ chose to petition the Supreme Court for review and certiorari was granted in *Jones*.[301] Perhaps DOJ expected the Court both to uphold the *Knotts* rule that "a person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another"[302] and to reject the mosaic theory outright due to the kind of chaotic legal landscape that could result if Fourth Amendment doctrine embraced some form of the mosaic theory. The reliance on *Knotts* in the Government's brief[303] and oral argument[304] would suggest this was their expectation and, at least for the time being, DOJ secured this very narrow result. But what DOJ may not have expected was a kind of clarity of vision from the Court with

---

[299] United States v. Maynard, 615 F.3d 544 (D.C. Cir. 2010).

[300] *Id.* at 562; *see also supra* Part II.B.

[301] *Maynard*, 615 F.3d at 544, *reh'g denied sub nom.* United States v. Jones, 625 F.3d 766 (D.C. Cir. 2010), *aff'd*, 132 S. Ct. 945 (2012).

[302] United States v. Knotts, 460 U.S. 276, 281 (1983)

[303] *See supra* note 9.

[304] *See supra* notes 1–2.

respect to the consequences of following DOJ down the path of simply affirming *Knotts*. At a legal symposium on the *Jones* case,[305] Antoine Jones's co-counsel, Professor Walter Dellinger, recounted[306] how he had described such consequences in an interview with Nina Totenberg:

> If the Supreme Court gave a green light to [warrantless GPS tracking, then] any officer can install any GPS device for any reason on anybody's car, even if the officer thinks it would be interesting to know where Supreme Court justices go at night when they leave the courthouse. No one would be immune from having GPS devices installed on their vehicles.[307]

Professor Dellinger went on to relate how that interview had aired the very morning of the *Jones* oral argument, at which Chief Justice Roberts' questioning included the hypothetical that led off this Article[308]—Dellinger's hypothetical—asking the Deputy Solicitor General whether the Government's theory permitted the tracking of Supreme Court Justices with GPS devices attached to their cars.[309] Professor Dellinger offered that he knew Jones had likely won his case when that question was asked, with "doctrine to follow"—whatever it might be.[310]

For now, the very specific morsel of doctrine that has followed from the majority opinion spared DOJ, for the time being, from the mosaic theory or a modern re-evaluation of the third party doctrine that could limit broad law enforcement access to non-content data.[311] Justice Scalia, with the assistance of Justice Sotomayor's vote, found a way to contain these issues and address government use of a GPS tracking device through a more limited trespass-based theory.[312] But Justice Scalia's exasperated, more than

---

[305] *North Carolina Journal of Law & Technology* Symposium: *U.S. v. Jones: Defining A Search in the 21st Century* (Jan. 25, 2013).

[306] Dellinger, *supra* note 146.

[307] Nina Totenberg, *Do Police Need Warrants For GPS Tracking Devices?* NPR (Nov. 8, 2011), http://m.npr.org/story/142032419.

[308] *See supra* text accompanying note 1.

[309] Dellinger, *supra* note 146.

[310] *Id.*

[311] *See supra* Part II.

[312] *See supra* Part II.

rhetorical question at oral argument, "Don't we have any legislatures out there that can stop this stuff?"[313] should serve notice upon DOJ about what a future case and changes or additions to Fourth Amendment doctrine could bring. Indeed, if DOJ had gone to the Court that morning expecting a friendly pro-law enforcement majority that would unequivocally endorse the logic of *Knotts,* Justice Scalia's message, though quietly uttered, should have had, for all who could interpret its import, the echoed force of Hamlet's words of rejection to Ophelia, another expectant but disappointed suitor—"DOJ: Get Thee to a Legislature."[314]

The arguments in the concurrences, on the other hand, do not so much echo the cruelty of Hamlet's rejection of Ophelia as his later ironic observation that he "must be cruel, only to be kind"[315] in berating his mother for marrying his Uncle Claudius less than a month after his father's death. If Justice Scalia's musings are subtle and measured, the concurrences are more urgent, perhaps threatening. The concurrences serve both to amplify Justice Scalia's hint and to identify the specific nature of the threat posed to law enforcement equities by continued reliance on the Court. Authored, as they are, by two Justices representative of the ideological poles of the current panel, they not only pointedly show DOJ that "the Justices of this Court"[316] will offer it no succor in this particular case, but they seem to foreclose the very possibility of any future positive relief in this venue by brandishing such bleak alternative solutions as a potential endorsement of some form of the mosaic theory or some yet unarticulated way of limiting or curtailing the third party doctrine, either of which could have damaging ramifications for law enforcement equities.[317] The message of the concurrences is not a note of paternal advice but, rather, one of stern warning. A future case with less containable

---

[313] Transcript of Oral Argument, *supra* note 1, at 26.

[314] "Get Thee to a Nunnery," WILLIAM SHAKESPEARE, HAMLET act 3, sc. 2, ll. 120–21.

[315] *Id.* at act 3, sc. 4, l. 178.

[316] *See* Statement of Deputy Solicitor General Michael Dreeben, Transcript of Oral Argument, *supra* note 1, at 9.

[317] *See supra* Part II.D.

facts could force Justice Scalia and his colleagues to render a more definitive, if much less palatable decision. Taken together, then, the opinions in *Jones* serve as a coordinated signal to DOJ that it should commit itself to the thorny path of the legislative process to avoid the consequences of any such, yet unarticulated, "doctrine to follow."