Readings for Session with Dan Richman & Matt Waxman
Columbia Law School

Please find attached three background documents:

1. Excerpts from *United States v. Jones*
2. Statement from FBI Director and Deputy Attorney General on "Going Dark"
3. Excerpts from Berkman Center report on Going Dark

Syllabus

NOTE: Where it is feasible, a syllabus (headnote) will be released, as is being done in connection with this case, at the time the opinion is issued. The syllabus constitutes no part of the opinion of the Court but has been prepared by the Reporter of Decisions for the convenience of the reader. See *United States* v. *Detroit Timber & Lumber Co.*, 200 U. S. 321, 337.

SUPREME COURT OF THE UNITED STATES

Syllabus

UNITED STATES *v.* JONES

CERTIORARI TO THE UNITED STATES COURT OF APPEALS FOR THE DISTRICT OF COLUMBIA CIRCUIT

No. 10–1259. Argued November 8, 2011—Decided January 23, 2012

The Government obtained a search warrant permitting it to install a Global-Positioning-System (GPS) tracking device on a vehicle registered to respondent Jones's wife. The warrant authorized installation in the District of Columbia and within 10 days, but agents installed the device on the 11th day and in Maryland. The Government then tracked the vehicle's movements for 28 days. It subsequently secured an indictment of Jones and others on drug trafficking conspiracy charges. The District Court suppressed the GPS data obtained while the vehicle was parked at Jones's residence, but held the remaining data admissible because Jones had no reasonable expectation of privacy when the vehicle was on public streets. Jones was convicted. The D. C. Circuit reversed, concluding that admission of the evidence obtained by warrantless use of the GPS device violated the Fourth Amendment.

Held: The Government's attachment of the GPS device to the vehicle, and its use of that device to monitor the vehicle's movements, constitutes a search under the Fourth Amendment. Pp. 3–12.

(a) The Fourth Amendment protects the "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." Here, the Government's physical intrusion on an "effect" for the purpose of obtaining information constitutes a "search." This type of encroachment on an area enumerated in the Amendment would have been considered a search within the meaning of the Amendment at the time it was adopted. Pp. 3–4.

(b) This conclusion is consistent with this Court's Fourth Amendment jurisprudence, which until the latter half of the 20th century was tied to common-law trespass. Later cases, which have deviated from that exclusively property-based approach, have applied the

Syllabus

analysis of Justice Harlan's concurrence in *Katz* v. *United States*, 389 U. S. 347, which said that the Fourth Amendment protects a person's "reasonable expectation of privacy," *id.*, at 360. Here, the Court need not address the Government's contention that Jones had no "reasonable expectation of privacy," because Jones's Fourth Amendment rights do not rise or fall with the *Katz* formulation. At bottom, the Court must "assur[e] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted." *Kyllo* v. *United States*, 533 U. S. 27, 34. *Katz* did not repudiate the understanding that the Fourth Amendment embodies a particular concern for government trespass upon the areas it enumerates. The *Katz* reasonable-expectation-of-privacy test has been added to, but not substituted for, the common-law trespassory test. See *Alderman* v. *United States*, 394 U. S. 165, 176; *Soldal* v. *Cook County*, 506 U. S. 56, 64. *United States* v. *Knotts*, 460 U. S. 276, and *United States* v. *Karo*, 468 U. S. 705—post-*Katz* cases rejecting Fourth Amendment challenges to "beepers," electronic tracking devices representing another form of electronic monitoring—do not foreclose the conclusion that a search occurred here. *New York* v. *Class*, 475 U. S. 106, and *Oliver* v. *United States*, 466 U. S. 170, also do not support the Government's position. Pp. 4–12.

(c) The Government's alternative argument—that if the attachment and use of the device was a search, it was a reasonable one—is forfeited because it was not raised below. P. 12.

615 F. 3d 544, affirmed.

SCALIA, J., delivered the opinion of the Court, in which ROBERTS, C. J., and KENNEDY, THOMAS, and SOTOMAYOR, JJ., joined. SOTOMAYOR, J., filed a concurring opinion. ALITO, J., filed an opinion concurring in the judgment, in which GINSBURG, BREYER, and KAGAN, JJ., joined.

SUPREME COURT OF THE UNITED STATES

No. 10–1259

UNITED STATES, PETITIONER *v.* ANTOINE JONES

ON WRIT OF CERTIORARI TO THE UNITED STATES COURT OF APPEALS FOR THE DISTRICT OF COLUMBIA CIRCUIT

[January 23, 2012]

JUSTICE SOTOMAYOR, concurring.

I join the Court's opinion because I agree that a search within the meaning of the Fourth Amendment occurs, at a minimum, "[w]here, as here, the Government obtains information by physically intruding on a constitutionally protected area." *Ante*, at 6, n. 3. In this case, the Government installed a Global Positioning System (GPS) tracking device on respondent Antoine Jones' Jeep without a valid warrant and without Jones' consent, then used that device to monitor the Jeep's movements over the course of four weeks. The Government usurped Jones' property for the purpose of conducting surveillance on him, thereby invading privacy interests long afforded, and undoubtedly entitled to, Fourth Amendment protection. See, *e.g.*, *Silverman* v. *United States*, 365 U. S. 505, 511–512 (1961).

Of course, the Fourth Amendment is not concerned only with trespassory intrusions on property. See, *e.g.*, *Kyllo* v. *United States*, 533 U. S. 27, 31–33 (2001). Rather, even in the absence of a trespass, "a Fourth Amendment search occurs when the government violates a subjective expectation of privacy that society recognizes as reasonable." *Id.*, at 33; see also *Smith* v. *Maryland*, 442 U. S. 735, 740–741 (1979); *Katz* v. *United States*, 389 U. S. 347, 361 (1967) (Harlan, J., concurring). In *Katz*, this Court enlarged its then-prevailing focus on property rights by announcing

that the reach of the Fourth Amendment does not "turn upon the presence or absence of a physical intrusion." *Id.*, at 353. As the majority's opinion makes clear, however, *Katz*'s reasonable-expectation-of-privacy test augmented, but did not displace or diminish, the common-law trespassory test that preceded it. *Ante*, at 8. Thus, "when the Government *does* engage in physical intrusion of a constitutionally protected area in order to obtain information, that intrusion may constitute a violation of the Fourth Amendment." *United States* v. *Knotts*, 460 U. S. 276, 286 (1983) (Brennan, J., concurring in judgment); see also, *e.g.*, *Rakas* v. *Illinois*, 439 U. S. 128, 144, n. 12 (1978). JUSTICE ALITO's approach, which discounts altogether the constitutional relevance of the Government's physical intrusion on Jones' Jeep, erodes that longstanding protection for privacy expectations inherent in items of property that people possess or control. See *post*, at 5–7 (opinion concurring in judgment). By contrast, the 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.

Nonetheless, as JUSTICE ALITO notes, physical intrusion is now unnecessary to many forms of surveillance. *Post*, at 9–12. With increasing regularity, the Government will be capable of duplicating the monitoring undertaken in this case by enlisting factory- or owner-installed vehicle tracking devices or GPS-enabled smartphones. See *United States* v. *Pineda-Moreno*, 617 F. 3d 1120, 1125 (CA9 2010) (Kozinski, C. J., dissenting from denial of rehearing en banc). In cases of electronic or other novel modes of surveillance that do not depend upon a physical invasion on property, the majority opinion's trespassory test may provide little guidance. But "[s]ituations involving merely the transmission of electronic signals without trespass

would *remain* subject to *Katz* analysis." *Ante,* at 11. As JUSTICE ALITO incisively observes, the same technological advances that have made possible nontrespassory surveillance techniques will also affect the *Katz* test by shaping the evolution of societal privacy expectations. *Post,* at 10–11. Under that rubric, I agree with JUSTICE ALITO that, at the very least, "longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy." *Post,* at 13.

In cases involving even short-term monitoring, some unique attributes of GPS surveillance relevant to the *Katz* analysis will require particular attention. GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations. See, *e.g., People* v. *Weaver*, 12 N. Y. 3d 433, 441–442, 909 N. E. 2d 1195, 1199 (2009) ("Disclosed in [GPS] data . . . will be trips the indisputably private nature of which takes little imagination to conjure: trips to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour motel, the union meeting, the mosque, synagogue or church, the gay bar and on and on"). The Government can store such records and efficiently mine them for information years into the future. *Pineda-Moreno,* 617 F. 3d, at 1124 (opinion of Kozinski, C. J.). And because GPS monitoring is cheap in comparison to conventional surveillance techniques and, by design, proceeds surreptitiously, it evades the ordinary checks that constrain abusive law enforcement practices: "limited police resources and community hostility." *Illinois* v. *Lidster*, 540 U. S. 419, 426 (2004).

Awareness that the Government may be watching chills associational and expressive freedoms. And the Government's unrestrained power to assemble data that reveal private aspects of identity is susceptible to abuse. The net

result is that 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." *United States* v. *Cuevas-Perez*, 640 F. 3d 272, 285 (CA7 2011) (Flaum, J., concurring).

I would take these attributes of GPS monitoring into account when considering the existence of a reasonable societal expectation of privacy in the sum of one's public movements. I would ask whether people reasonably expect that their movements will be recorded and aggregated in a manner that enables the Government to ascertain, more or less at will, their political and religious beliefs, sexual habits, and so on. I do not regard as dispositive the fact that the Government might obtain the fruits of GPS monitoring through lawful conventional surveillance techniques. See *Kyllo*, 533 U. S., at 35, n. 2; *ante*, at 11 (leaving open the possibility that duplicating traditional surveillance "through electronic means, without an accompanying trespass, is an unconstitutional invasion of privacy"). I would also consider the appropriateness of entrusting to the Executive, in the absence of any oversight from a coordinate branch, a tool so amenable to misuse, especially in light of the Fourth Amendment's goal to curb arbitrary exercises of police power to and prevent "a too permeating police surveillance," *United States* v. *Di Re*, 332 U. S. 581, 595 (1948).*

---

* *United States* v. *Knotts*, 460 U. S. 276 (1983), does not foreclose the conclusion that GPS monitoring, in the absence of a physical intrusion, is a Fourth Amendment search. As the majority's opinion notes, *Knotts* reserved the question whether "'different constitutional principles may be applicable'" to invasive law enforcement practices such as GPS tracking. See *ante*, at 8, n. 6 (quoting 460 U. S., at 284).

United States v. *Karo*, 468 U. S. 705 (1984), addressed the Fourth

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. *E.g., Smith*, 442 U. S., at 742; *United States* v. *Miller*, 425 U. S. 435, 443 (1976). This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks. 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. Perhaps, as JUSTICE ALITO notes, some people may find the "tradeoff" of privacy for convenience "worthwhile," or come to accept this "diminution of privacy" as "inevitable," *post*, at 10, and perhaps not. I for one doubt that people would accept without complaint the warrantless disclosure to the Government of a list of every Web site they had visited in the last week, or month, or year. But whatever the societal expectations, they can attain constitutionally protected status only if our Fourth Amendment jurisprudence ceases

---

Amendment implications of the installation of a beeper in a container with the consent of the container's original owner, who was aware that the beeper would be used for surveillance purposes. *Id.*, at 707. Owners of GPS-equipped cars and smartphones do not contemplate that these devices will be used to enable covert surveillance of their movements. To the contrary, subscribers of one such service greeted a similar suggestion with anger. Quain, Changes to OnStar's Privacy Terms Rile Some Users, N. Y. Times (Sept. 22, 2011), online at http://wheels.blogs.nytimes.com/2011/09/22/changes-to-onstars-privacy-terms-rile-some-users (as visited Jan. 19, 2012, and available in Clerk of Court's case file). In addition, the bugged container in *Karo* lacked the close relationship with the target that a car shares with its owner. The bugged container in *Karo* was stationary for much of the Government's surveillance. See 468 U. S., at 708–710. A car's movements, by contrast, are its owner's movements.

to treat secrecy as a prerequisite for privacy. I would not assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection. See *Smith*, 442 U. S., at 749 (Marshall, J., dissenting) ("Privacy is not a discrete commodity, possessed absolutely or not at all. Those who disclose certain facts to a bank or phone company for a limited business purpose need not assume that this information will be released to other persons for other purposes"); see also *Katz*, 389 U. S., at 351–352 ("[W]hat [a person] seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected").

Resolution of these difficult questions in this case is unnecessary, however, because the Government's physical intrusion on Jones' Jeep supplies a narrower basis for decision. I therefore join the majority's opinion.

SUPREME COURT OF THE UNITED STATES

No. 10–1259

UNITED STATES, PETITIONER *v.* ANTOINE JONES

ON WRIT OF CERTIORARI TO THE UNITED STATES COURT OF APPEALS FOR THE DISTRICT OF COLUMBIA CIRCUIT

[January 23, 2012]

JUSTICE ALITO, with whom JUSTICE GINSBURG, JUSTICE BREYER, and JUSTICE KAGAN join, concurring in the judgment.

Amendment, do these recent decisions represent a change in the law or simply the application of the old tort to new situations?

IV

A

The *Katz* expectation-of-privacy test avoids the problems and complications noted above, but it is not without its own difficulties. It involves a degree of circularity, see *Kyllo*, 533 U. S., at 34, and judges are apt to confuse their own expectations of privacy with those of the hypothetical reasonable person to which the *Katz* test looks. See *Minnesota* v. *Carter*, 525 U. S. 83, 97 (1998) (SCALIA, J., concurring). In addition, the *Katz* test rests on the assumption that this hypothetical reasonable person has a well-developed and stable set of privacy expectations. But technology can change those expectations. Dramatic technological change may lead to periods in which popular expectations are in flux and may ultimately produce significant changes in popular attitudes. New technology may provide increased convenience or security at the expense of privacy, and many people may find the tradeoff worthwhile. And even if the public does not welcome the diminution of privacy that new technology entails, they may eventually reconcile themselves to this development as inevitable.[6]

On the other hand, concern about new intrusions on privacy may spur the enactment of legislation to protect against these intrusions. This is what ultimately happened with respect to wiretapping. After *Katz*, Congress

---

[6]See, *e.g.*, NPR, The End of Privacy http://www.npr.org/series/114250076/the-end-of-privacy (all Internet materials as visited Jan. 20, 2012, and available in Clerk of Court's case file); Time Magazine, Everything About You Is Being Tracked—Get Over It, Joel Stein, Mar. 21, 2011, Vol. 177, No. 11.

did not leave it to the courts to develop a body of Fourth Amendment case law governing that complex subject. Instead, Congress promptly enacted a comprehensive statute, see 18 U. S. C. §§2510–2522 (2006 ed. and Supp. IV), and since that time, the regulation of wiretapping has been governed primarily by statute and not by case law.[7] In an ironic sense, although *Katz* overruled *Olmstead*, Chief Justice Taft's suggestion in the latter case that the regulation of wiretapping was a matter better left for Congress, see 277 U. S., at 465–466, has been borne out.

B

Recent years have seen the emergence of many new devices that permit the monitoring of a person's movements. 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.[8] For older phones, the accuracy of the location information depends on the density of the tower network, but new "smart phones," which

---

[7]See Kerr, The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution, 102 Mich. L. Rev. 801, 850–851 (2004) (hereinafter Kerr).

[8]See CTIA Consumer Info, 50 Wireless Quick Facts, http://www.ctia.org/consumer_info/index.cfm/AID/10323.

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.[9] Similarly, phone-location-tracking services are offered as "social" tools, allowing consumers to find (or to avoid) others who enroll in these services. The availability and use of these and other new devices will continue to shape the average person's expectations about the privacy of his or her daily movements.

V

In the pre-computer age, the greatest protections of privacy were neither constitutional nor statutory, but practical. Traditional surveillance for any extended period of time was difficult and costly and therefore rarely undertaken. The surveillance at issue in this case—constant monitoring of the location of a vehicle for four weeks—would have required a large team of agents, multiple vehicles, and perhaps aerial assistance.[10] Only an investigation of unusual importance could have justified such an

---

[9]See, *e.g.*, The bright side of sitting in traffic: Crowdsourcing road congestion data, Google Blog, http://googleblog.blogspot.com/2009/08/bright-side-of-sitting-in-traffic.html.

[10]Even with a radio transmitter like those used in *United States* v. *Knotts*, 460 U. S. 276 (1983), or *United States* v. *Karo*, 468 U. S. 705 (1984), such long-term surveillance would have been exceptionally demanding. The beepers used in those cases merely "emit[ted] periodic signals that [could] be picked up by a radio receiver." *Knotts*, 460 U.S., at 277. The signal had a limited range and could be lost if the police did not stay close enough. Indeed, in *Knotts* itself, officers lost the signal from the beeper, and only "with the assistance of a monitoring device located in a helicopter [was] the approximate location of the signal . . . picked up again about one hour later." *Id.*, at 278.

expenditure of law enforcement resources. Devices like the one used in the present case, however, make long-term monitoring relatively easy and cheap. In circumstances involving dramatic technological change, the best solution to privacy concerns may be legislative. See, *e.g.*, Kerr, 102 Mich. L. Rev., at 805–806. A legislative body is well situated to gauge changing public attitudes, to draw detailed lines, and to balance privacy and public safety in a comprehensive way.

To date, however, Congress and most States have not enacted statutes regulating the use of GPS tracking technology for law enforcement purposes. The best that we can do in this case is to apply existing Fourth Amendment doctrine and to ask whether the use of GPS tracking in a particular case involved a degree of intrusion that a reasonable person would not have anticipated.

Under this approach, relatively short-term monitoring of a person's movements on public streets accords with expectations of privacy that our society has recognized as reasonable. See *Knotts*, 460 U. S., at 281–282. But the use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy. For such offenses, society's expectation has been that law enforcement agents and others would not—and indeed, in the main, simply could not—secretly monitor and catalogue every single movement of an individual's car for a very long period. In this case, for four weeks, law enforcement agents tracked every movement that respondent made in the vehicle he was driving. We need not identify with precision the point at which the tracking of this vehicle became a search, for the line was surely crossed before the 4-week mark. Other cases may present more difficult questions. But where uncertainty exists with respect to whether a certain period of GPS surveil

lance is long enough to constitute a Fourth Amendment search, the police may always seek a warrant.[11] We also need not consider whether prolonged GPS monitoring in the context of investigations involving extraordinary offenses would similarly intrude on a constitutionally protected sphere of privacy. In such cases, long-term tracking might have been mounted using previously available techniques.

* * *

For these reasons, I conclude that the lengthy monitoring that occurred in this case constituted a search under the Fourth Amendment. I therefore agree with the majority that the decision of the Court of Appeals must be affirmed.

---

[11] In this case, the agents obtained a warrant, but they did not comply with two of the warrant's restrictions: They did not install the GPS device within the 10-day period required by the terms of the warrant and by Fed. Rule Crim. Proc. 41(e)(2)(B)(i), and they did not install the GPS device within the District of Columbia, as required by the terms of the warrant and by 18 U. S. C. §3117(a) and Rule 41(b)(4). In the courts below the Government did not argue, and has not argued here, that the Fourth Amendment does not impose these precise restrictions and that the violation of these restrictions does not demand the suppression of evidence obtained using the tracking device. See, *e.g.*, *United States* v. *Gerber*, 994 F. 2d 1556, 1559–1560 (CA11 1993); *United States* v. *Burke*, 517 F. 2d 377, 386–387 (CA2 1975). Because it was not raised, that question is not before us.

James B. Comey
Director
Federal Bureau of Investigation

Joint Statement with Deputy Attorney General Sally Quillian Yates Before the Senate Judiciary Committee
Washington, D.C.
July 8, 2015

Going Dark: Encryption, Technology, and the Balances Between Public Safety and Privacy

Good morning, Chairman Grassley, Ranking Member Leahy, and members of the Judiciary Committee. Thank you for the opportunity to testify today about the growing challenges to public safety and national security that have eroded our ability to obtain electronic information and evidence pursuant to a court order or warrant. We in law enforcement often refer to this problem as "Going Dark."

We would also like to thank this committee more generally for its continued support for the mission of the Department of Justice. We know that you, like us, take very seriously the role of the Department in protecting the public in a manner that upholds the Constitution and the rule of law.

Introduction

In recent years, new methods of electronic communication have transformed our society, most visibly by enabling ubiquitous digital communications and facilitating broad e-commerce. As such, it is important for our global economy and our national security to have strong encryption standards. The development and robust adoption of strong encryption is a key tool to secure commerce and trade, safeguard private information, promote free expression and association, and strengthen cyber security. The Department is on the frontlines of the fight against cyber crime, and

we know first-hand the damage that can be caused by those who exploit vulnerable and insecure systems. We support and encourage the use of secure networks to prevent cyber threats to our critical national infrastructure, our intellectual property, and our data so as to promote our overall safety.

American citizens care deeply about privacy, and rightly so. Many companies have been responding to a market demand for products and services that protect the privacy and security of their customers. This has generated positive innovation that has been crucial to the digital economy. We, too, care about these important principles. Indeed, it is our obligation to uphold civil liberties, including the right to privacy.

We have always respected the fundamental right of people to engage in private communications, regardless of the medium or technology. Whether it is instant messages, texts, or old-fashioned letters, citizens have the right to communicate with one another in private without unauthorized government surveillance—not simply because the Constitution demands it, but because the free flow of information is vital to a thriving democracy.

The benefits of our increasingly digital lives, however, have been accompanied by new dangers, and we have been forced to consider how criminals and terrorists might use advances in technology to their advantage. For example, malicious actors can take advantage of the Internet to covertly plot violent robberies, murders, and kidnappings; sex offenders can establish virtual communities to buy, sell, and encourage the creation of new depictions of horrific sexual abuse of children; and individuals, organized criminal networks, and nation-states can exploit weaknesses in our cyber-defenses to steal our sensitive, personal information. Investigating and prosecuting these offenders is a core responsibility and priority of the Department of Justice. As national security and criminal threats continue to evolve, the Department has worked hard to stay ahead of changing threats and changing technology.

We must ensure both the fundamental right of people to engage in private communications as well as the protection of the public. One of the bedrock principles upon which we rely to guide us is the principle of judicial authorization: that if an independent judge finds reason to believe that certain private

communications contain evidence of a crime, then the government can conduct a limited search for that evidence. For example, by having a neutral arbiter—the judge—evaluate whether the government's evidence satisfies the appropriate standard, we have been able to protect the public and safeguard citizens' Constitutional rights.

The Department of Justice has been and will always be committed to protecting the liberty and security of those whom we serve. In recent months, however, we have on a new scale seen mainstream products and services designed in a way that gives users sole control over access to their data. As a result, law enforcement is sometimes unable to recover the content of electronic communications from the technology provider even in response to a court order or duly-authorized warrant issued by a federal judge. For example, many communications services now encrypt certain communications by default, with the key necessary to decrypt the communications solely in the hands of the end user. This applies both when the data is "in motion" over electronic networks, or "at rest" on an electronic device. If the communications provider is served with a warrant seeking those communications, the provider cannot provide the data because it has designed the technology such that it cannot be accessed by any third party.

Threats

The more we as a society rely on electronic devices to communicate and store information, the more likely it is that information that was once found in filing cabinets, letters, and photo albums will now be stored only in electronic form. We have seen case after case—from homicides and kidnappings, to drug trafficking, financial fraud, and child exploitation—where critical evidence came from smart phones, computers, and online communications.

When changes in technology hinder law enforcement's ability to exercise investigative tools and follow critical leads, we may not be able to identify and stop terrorists who are using social media to recruit, plan, and execute an attack in our country. We may not be able to root out the child predators hiding in the shadows of the Internet, or find and arrest violent criminals who are targeting our neighborhoods. We may not be able to recover critical information from a device that belongs to a victim who cannot provide us with the password, especially when

time is of the essence.

These are not just theoretical concerns. We continue to identify individuals who seek to join the ranks of foreign fighters traveling in support of the Islamic State of Iraq and the Levant, commonly known as ISIL, and also homegrown violent extremists who may aspire to attack the United States from within. These threats remain among the highest priorities for the Department of Justice, including the FBI, and the United States government as a whole.

Of course, encryption is not the only technology terrorists and criminals use to further their ends. Terrorist groups, such as ISIL, use the Internet to great effect. With the widespread horizontal distribution of social media, terrorists can spot, assess, recruit, and radicalize vulnerable individuals of all ages in the United States either to travel or to conduct a homeland attack. As a result, foreign terrorist organizations now have direct access into the United States like never before. For example, in recent arrests, a group of individuals was contacted by a known ISIL supporter who had already successfully traveled to Syria and encouraged them to do the same. Some of these conversations occur in publicly accessed social networking sites, but others take place via private messaging platforms. These encrypted direct messaging platforms are tremendously problematic when used by terrorist plotters.

Outside of the terrorism arena we see countless examples of the impact changing technology is having on our ability to affect our court authorized investigative tools. For example, last December a long-haul trucker kidnapped his girlfriend, held her in his truck, drove her from state to state and repeatedly sexually assaulted her. She eventually escaped and pressed charges for sexual assault and kidnapping. The trucker claimed that the woman he had kidnapped engaged in consensual sex. The trucker in this case happened to record his assault on video using a smartphone, and law enforcement was able to access the content stored on that phone pursuant to a search warrant, retrieving video that revealed that the sex was not consensual. A jury subsequently convicted the trucker.

In a world where users have sole control over access to their devices and communications, and so can easily block all lawfully authorized access to their data, the jury would not have been able to consider that evidence, unless the truck

driver, against his own interest, provided the data. And the theoretical availability of other types of evidence, irrelevant to the case, would have made no difference. In that world, the grim likelihood that he would go free is a cost that we must forthrightly acknowledge and consider.

We are seeing more and more cases where we believe significant evidence resides on a phone, a tablet, or a laptop—evidence that may be the difference between an offender being convicted or acquitted. If we cannot access this evidence, it will have ongoing, significant impacts on our ability to identify, stop, and prosecute these offenders.

Legal Framework

We would like to emphasize that the Going Dark problem is, at base, one of technological choices and capability. We are not asking to expand the government's surveillance authority, but rather we are asking to ensure that we can continue to obtain electronic information and evidence pursuant to the legal authority that Congress has provided to us to keep America safe.

The rules for the collection of the content of communications in order to protect public safety have been worked out by Congress and the courts over decades. Our country is justifiably proud of the strong privacy protections established by the Constitution and by Congress, and the Department of Justice fully complies with those protections. The core question is this: Once all of the requirements and safeguards of the laws and the Constitution have been met, are we comfortable with technical design decisions that result in barriers to obtaining evidence of a crime?

We would like to describe briefly the law and the extensive checks, balances, and safeguards that it contains. In addition to the Constitution, two statutes are particularly relevant to the Going Dark problem. Generally speaking, in order for the government to conduct *real-time—i.e.*, data in motion—electronic surveillance of the content of a suspect's communications, it must meet the standards set forth in either the amended versions of Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (often referred to as "Title III" or the "Wiretap Act") or the Foreign Intelligence Surveillance Act of 1978 (or "FISA"). Title III authorizes the government to obtain a court order to conduct surveillance of wire, oral, or

electronic communications when it is investigating federal felonies. Generally speaking, FISA similarly relies upon judicial authorization, through the Foreign Intelligence Surveillance Court (FISC), to approve surveillance directed at foreign intelligence and international terrorism threats. Regardless of which statute governs, however, the standards for the real-time electronic surveillance of United States persons' communications are demanding. For instance, if federal law enforcement seeks the authority to intercept phone calls in a criminal case using the Wiretap Act, a federal district court judge must find:

- That there is probable cause to believe the person whose communications are targeted for interception is committing, has committed, or is about to commit, a felony offense;
- That alternative investigative procedures have failed, are unlikely to succeed, or are too dangerous; and
- That there is probable cause to believe that evidence of the felony will be obtained through the surveillance.

The law also requires that before an application is even brought to a court, it must be approved by a high-ranking Department of Justice official. In addition, court orders allowing wiretap authority expire after 30 days; if the government seeks to extend surveillance beyond this period, it must submit another application with a fresh showing of probable cause and investigative necessity. And the government is required to minimize to the extent possible its electronic interceptions to exclude non-pertinent and privileged communications. All of these requirements are approved by a federal court.

The statutory requirements for electronic surveillance of U.S. persons under FISA are also demanding. To approve that surveillance, the FISC, must, among other things, find probable cause to believe:

- That the target of the surveillance is a foreign power or agent of a foreign power; and
- That each of the facilities or places at which the electronic surveillance is directed is being used or is about to be used by a foreign power or an agent of a foreign power.

Similarly, when law enforcement investigators seek access to electronic information

stored—i.e., data at rest—on a device, such as a smartphone, they are likewise bound by the mandates of the Fourth Amendment, which typically require them to demonstrate probable cause to a neutral judge, who independently decides whether to issue a search warrant for that data.

Collectively, these statutes reflect a concerted Congressional effort, overseen by an independent judiciary, to validate the principles enshrined in our Constitution and balance several sometimes competing, yet equally legitimate social interests: privacy, public safety, national security, and effective justice. The evolution and operation of technology today has led to recent trends that threaten this time-honored approach. In short, the same ingenuity that has improved our lives in so many ways has also resulted in the proliferation of products and services where providers can no longer assist law enforcement in executing warrants.

Provider Assistance

BothTitle III and FISA include provisions mandating technical assistance so that the government will be able to carry out activities authorized by the court. For example, Title III specifies that a "service provider, landlord...or other person shall furnish [the government]...forthwith all...technical assistance necessary to accomplish the interception." As the communications environment has grown in volume and complexity, technical assistance has proven to be essential for interception to occur. These provisions alone, however, have not historically been sufficient to enable the government to conduct electronic surveillance in a timely and effective manner.

In the early 1990s, the telecommunications industry was undergoing a major transformation and the government faced a similar problem: determining how best to ensure that law enforcement could reliably obtain evidence from emerging telecommunications networks. At that time, law enforcement agencies were experiencing a reduced ability to conduct intercepts of mobile voice communications as digital, switch-based telecommunications services grew in popularity. In response, Congress enacted the Communications Assistance for Law Enforcement Act (CALEA) in 1994. CALEA requires "telecommunications carriers" to develop and deploy intercept solutions in their networks to ensure that the government is able to intercept electronic communications when lawfully authorized, although it does not require a carrier to decrypt communications

encrypted by the customer unless the carrier provided the encryption and possesses the information necessary to decrypt. Specifically, it requires carriers to be able to isolate and deliver particular communications, to the exclusion of other communications, and to be able to deliver information regarding the origination and termination of the communication (also referred to as "pen register information" or "dialing and signaling information"). CALEA regulates the capabilities that covered entities must have and does not affect the process or the legal standards that the government must meet in order to obtain a court order to collect communications or related data.

While CALEA was intended to keep pace with technological changes, its focus was on telecommunications carriers that provided traditional telephony and mobile telephone services, not Internet-based communications services. Over the years, through interpretation of the statute by the Federal Communications Commission, the reach of CALEA has been expanded to include facilities-based broadband Internet access and Voice over Internet Protocol (VoIP) services that are fully interconnected with the public switched telephone network. Although that expansion of coverage has been extremely helpful, CALEA does not cover popular Internet-based communications services such as e-mail, Internet messaging, social networking sites, or peer-to-peer services.

At the time CALEA was enacted, Internet-based communications were in a fairly early stage of development, and digital telephony represented the greatest challenge to law enforcement. However, due to the revolutionary shift in communications technology in recent years, the government has lost ground in its ability to execute court orders with respect to Internet-based communications that are not covered by CALEA.

The harms resulting from the inability of companies to comply with court-ordered surveillance warrants are not abstract, and have very real consequences in different types of criminal and national security investigations.

Going Forward

Mr. Chairman, The Department of Justice believes that the challenges posed by the Going Dark problem are grave, growing, and extremely complex. At the outset, it is important to emphasize that we believe that there is no one-size-fits-all strategy that

will ensure progress. We have been asked what we should do going forward. We believe we will need to pursue multiple paths:

All involved must continue to ensure that citizens' legitimate privacy interests can be effectively secured, including through robust technology and legal protections.

We must continue the current public debate about how best to ensure that privacy and security can co-exist and reinforce each other, and continue to consider all of the legitimate concerns at play, including ensuring that law enforcement can keep us safe. The debate so far has been a challenging and highly charged discussion, but one that we believe is essential to have. This includes a productive and meaningful dialogue on how encryption as currently implemented poses real barriers to law enforcement's ability to seek information in specific cases of possible national security threat.

We also cannot lose sight of the international implications of this issue. It is clear that governments across the world, including those of our closest allies, recognize the serious public safety risks if criminals can plan and undertake illegal acts without fear of detection. It is also true that other countries—particularly those without our commitment to the rule of law—are using this debate as a cynical means to create trade barriers, impose undue burdens on our companies, and undermine human rights. We should be clear that any steps that we take here in the United States may impact the decisions that other nations take—both our closest democratic allies and more repressive regimes. In addition, any next steps we identify will be more effective if we are working together with our allies, and made more difficult if we are isolated.

We should also continue to invest in developing tools, techniques, and capabilities designed to mitigate the increasing technical challenges associated with the Going Dark problem. In limited circumstances, this investment may help mitigate the risks posed in high priority national security or criminal cases, although it will most likely be unable to provide a timely or scalable solution in terms of addressing the full spectrum of public safety needs.

We don't have any silver bullet, and the discussions within the Executive Branch are still ongoing. While there has not yet been a decision whether to seek legislation, we must work with Congress, industry, academics, privacy groups and

others to craft an approach that addresses all of the multiple, competing legitimate concerns that have been the focus of so much debate in recent months. But we can all agree that we will need ongoing honest and informed public debate about how best to protect liberty and security in both our laws and our technology.

Conclusion

Mr. Chairman and Ranking Member Leahy, we would like to thank you and the members of this committee again for your attention to this subject of national importance. While technology may change, our basic commitment at the Department to upholding the rule of law and our constitutional traditions does not. Our goal at the Department is to work collaboratively and in good faith with interested stakeholders to explore approaches that protect the integrity of technology and promote strong encryption to protect privacy, while still allowing lawful access to information in order to protect public safety and national security.

We would be happy to answer any questions that you may have.

Berkman

The Berkman Center for Internet & Society
at Harvard University

Don't Panic

Making Progress on the "Going Dark" Debate

February 1, 2016

Introduction

In the last year, conversations around surveillance have centered on the use of encryption in communications technologies. The decisions of Apple, Google, and other major providers of communications services and products to enable end-to-end encryption in certain applications, on smartphone operating systems, as well as default encryption of mobile devices, at the same time that terrorist groups seek to use encryption to conceal their communication from surveillance, has fueled this debate.

The U.S. intelligence and law enforcement communities view this trend with varying degrees of alarm, alleging that their interception capabilities are "going dark." As they describe it, companies are increasingly adopting technological architectures that inhibit the government's ability to obtain access to communications, even in circumstances that satisfy the Fourth Amendment's warrant requirements. Encryption is the hallmark of these architectures. Government officials are concerned because, without access to communications, they fear they may not be able to prevent terrorist attacks and investigate and prosecute criminal activity. Their solution is to force companies to maintain access to user communications and data, and provide that access to law enforcement on demand, pursuant to the applicable legal process. However, the private sector has resisted. Critics fear that architectures geared to guarantee such access would compromise the security and privacy of users around the world, while also hurting the economic viability of U.S. companies. They also dispute the degree to which the proposed solutions would truly prevent terrorists and criminals from communicating in mediums resistant to surveillance.

Leading much of the debate on behalf of the U.S. government is the Department of Justice, including the Federal Bureau of Investigation, whose leaders have commented on the matter in numerous public statements, speeches, and Congressional testimony throughout 2014 and 2015. After nearly a year of discourse, which included numerous statements critical of the government's position from former U.S. intelligence officials and security technologists, the White House declared in October 2015 it would not pursue a legislative fix in the near future.[1]

However, this decision has not brought closure. The FBI has since focused its energy on encouraging companies to voluntarily find solutions that address the investigative concerns. Most recently, terrorist attacks in San Bernardino, Paris, and elsewhere around the world, along with rising concern about the terrorist group ISIS, have focused increased attention on the issues of surveillance and encryption. These developments have led to renewed calls, including among U.S. Presidential candidates, for the government and private sector to work together on the going dark issue and for the Obama administration to reconsider its position.

Findings

Although we were not able to unanimously agree upon the scope of the problem or the policy solution that would strike the best balance, we take the warnings of the FBI and others at face value: conducting certain types of surveillance has, to some extent, become more difficult in light of technological changes. Nevertheless, we question whether the "going dark" metaphor accurately describes the state of affairs. Are we really headed to a future in which our ability to effectively surveil criminals and bad actors is impossible? We think not.

Short of a form of government intervention in technology that appears contemplated by no one outside of the most despotic regimes, communication channels resistant to surveillance will always exist. This is especially true given the generative nature of the modern Internet, in which new services and software can be made available without centralized vetting. However, the question we explore is the significance of this lack of access to communications for legitimate government interests. We argue that communications in the future will neither be eclipsed into darkness nor illuminated without shadow. Market forces and commercial interests will likely limit the circumstances in which companies will offer encryption that obscures user data from the companies themselves, and the trajectory of technological development points to a future abundant in unencrypted data, some of which can fill gaps left by the very communication channels law enforcement fears will "go dark" and beyond reach.

In short, our findings are:

- End-to-end encryption and other technological architectures for obscuring user data are unlikely to be adopted ubiquitously by companies, because the majority of businesses that provide communications services rely on access to user data for revenue streams and product functionality, including user data recovery should a password be forgotten.
- Software ecosystems tend to be fragmented. In order for encryption to become both widespread and comprehensive, far more coordination and standardization than currently exists would be required.
- Networked sensors and the Internet of Things are projected to grow substantially, and this has the potential to drastically change surveillance. The still images, video, and audio captured by these devices may enable real-time intercept and recording with after-the-fact access. Thus an inability to monitor an encrypted channel could be mitigated by the ability to monitor from afar a person through a different channel.
- Metadata is not encrypted, and the vast majority is likely to remain so. This is data that needs to stay unencrypted in order for the systems to operate: location data from cell phones and other devices, telephone calling records, header information in e-mail, and so on. This information provides an enormous amount of surveillance data that was unavailable before these systems became widespread.
- These trends raise novel questions about how we will protect individual privacy and security in the future. Today's debate is important, but for all its efforts to take account of technological trends, it is largely taking place without reference to the full picture.

A Catalyst: Apple, Google, and Others Introduce Easy-to-Use, Built-In Encryption

In September 2014, about a year and a half after the disclosures by former NSA contractor Edward Snowden, Apple announced its decision to include default encryption of the password-protected contents of its devices in the then-next version of its mobile operating systems, iOS 8.[2] Indeed, data generated by many of the system apps on iOS 8 and later versions are encrypted when data is stored locally on the phone, in transit, and stored on Apple's servers.[3] The decryption keys are tied to the device password and only stored locally on the phone.

Not long after Apple's announcement, Google followed suit by announcing that Lollipop, its next version of Android OS, would enable device encryption by default.[4] Then, in November 2014, WhatsApp, the

popular instant messaging service for smartphones now owned by Facebook, announced it would support TextSecure, an end-to-end encryption protocol.[5] In March 2015, Yahoo introduced source code for an extension that encrypts messages in Yahoo Mail, though it requires users to run a key exchange server.[6] These steps bring to the appliance-style mobile world some of the technologies that have long been available – if not enabled by default – for personal computing operating systems, such as Apple's FileVault and Microsoft's Bitlocker.

The most significant aspects of these announcements are that the encryption takes place using keys solely in the possession of the respective device holders, and it is enabled by default.

While the going dark problem encompasses a range of architectural changes that impede government access, the adoption of encryption of data at rest, and end-to-end encryption in some common communications applications, by companies has become a focal point in the current debate, particularly those in which service providers do not have access to the keys. For example, *end-to-end* encryption is being used to describe scenarios in which information is being encrypted at the end points of a communication channel, and only the original sender and intended recipient possess the keys necessary to decrypt the message. In other words, the information is (in theory, and as advertised) not capable of being read by anyone who sees it traverse a network between the sender and the receiver, including an intermediary service provider, such as Apple. Similarly, *device* encryption – in which the keys exist only on locked devices – prevents the contents from being read by anyone who does not possess the keys.

The distinction is important because an overwhelming percentage of Internet users communicate through web-based services, such as webmail, instant messages, and social networking websites that are not end-to-end encrypted. In the course of an investigation, government officials can intercept communications and seek access to stored communications held by these intermediaries by obtaining a warrant, court order, or subpoena, provided that the company is capable of producing the information sought. However, without access to the keys, a company like Apple is incapable of providing a means to access communications in transit or stored on the company's services, regardless of whether law enforcement presents a valid warrant or court order.[7]

The role of default options and native support for encryption is also important. As with Filevault and Bitlocker for their data at rest, individuals have been able to use encryption software to send and receive end-to-end encrypted messages for a long time. For example, the first widely available public-key crypto software, Pretty Good Privacy (PGP), was made available to the public in the early 1990s. However, for the average computer user, e-mail encryption software has proven difficult to use, especially when it is not supported natively by communication software.[8] There is a well-documented learning curve to using the

software and it adds several steps to sending messages – both the sender and the recipient need to understand the encryption process, possess the software, generate a key pair, share the public keys, and encrypt and decrypt the messages. Much of this adds complexity and friction that is simply too much for most users to bother.

The complexity is substantially reduced when encryption is supported natively by communication software. When encryption is seamlessly integrated, a user does not have to take any affirmative actions to encrypt or decrypt messages, and much of the process occurs on the back end of the software. In fact, an average user might not be able to tell the difference between an encrypted message and an unencrypted message. When these options are enabled by default on popular devices and platforms, like the iPhone, a large swath of communications is encrypted.[9] Up to this point, government officials have not had to worry about the widespread use of such encryption, but the default nature of these schemes could alter the landscape. To be sure, in the past there was simply less data for government officials to seek in the first place – the amount of digital communications taking place in the PC-only era from 1977 to 2007 – even with the rise of the Internet in between – is dwarfed by the communications facilitated by mobile devices.

Despite all the noise, few of the headline-grabbing and anxiety-provoking (for government, at least) moves by device and operating system makers from 2014 have materialized into real-world default encryption that is beyond the reach of government actors.[10] Moreover, as we explore below, for a variety of reasons, it is not clear that the wave of encryption introduced in recent years will continue.

The "Going Dark" Debate Begins (Again)

This is not the first debate about the public's ability to use encryption and the government's ability to access communications. Often recounted as the "crypto wars," government access to encrypted communications has been the subject of hot debate and restrictive policy since the 1970s, with the government ultimately relaxing many export-control restrictions on software containing strong cryptographic algorithms in 2000.[11] The roles and obligations of telecommunications companies in providing a means for government actors to wiretap voice communications – in particular on the legacy telephone system that predated the PC and Internet era – have also been debated extensively over these decades. This was framed in the U.S. by the Communications Assistance to Law Enforcement Act – CALEA – which required telephone companies and others to ensure that their networks could be wiretapped, with appropriate legal process, as network technologies moved from analog to digital.[12]

The FBI has led the government's participation in the current debate. The Bureau started publicly raising concerns in 2010 about its ability to capture online communications.[13] The FBI's then-General Counsel,

Valerie Caproni, appeared before the Senate Judiciary Committee and used the phrase "going dark" to characterize the concern, citing a widening gap between law enforcement's legal privilege to intercept electronic communications and its practical ability to actually intercept those communications.[14] Her testimony emphasized that many Internet-based communications services have not only become more complex but have also deployed in modalities that are not subject to the Communications Assistance to Law Enforcement Act.[15] Other reports with similar accounts surfaced during this time period as well, including a declassified FBI situational report on cyber activity that described how data can be "hidden" from law enforcement by using encryption and the end points of communications channels can be obfuscated through use of proxies such as the Tor network.[16]

While the FBI has been the most vocal government agency about this issue,[17] foreign intelligence agencies such as the Central Intelligence Agency and National Security Agency also face obstacles due to encryption and other architectures that impede their access. The government is not a monolithic organization, and the encryption debate is not viewed the same way across governmental organizations or among the individuals within these organizations. The needs and resources of government organizations differ, as do their jurisdictional ambits. For instance, the resources available to the FBI for defeating encryption may be fewer than those available to the NSA. Likewise, state and local authorities have access to fewer resources than law enforcement operating at the federal level. However, while the degree of concern and operational value may not be shared across different agencies and levels of government, there is a general sense by actors within both the intelligence and law enforcement communities that, were all else equal, they would benefit if technological architectures did not present a barrier to investigations. (To be sure, all else is not equal – for example, if all communications were routinely unencrypted, citizens would be exposed to surveillance from myriad sources, many of whom might be viewed as national security threats by those citizens' governments.) Meanwhile certain agencies, including the Department of State, the Naval Research Laboratories, and the Defense Advanced Research Projects Agency (DARPA) have helped support the development of the Tor network, which hides the transactional information of Web-based communications. There are security reasons as well as human-rights interests for the U.S. government's support of Tor.

Since Caproni's invocation of the going dark metaphor in 2010, the problem, according to government officials, continues to worsen. Encryption has become central to their concerns. FBI Director James Comey, who has perhaps been the most vocal government official on this topic throughout the last year, highlighted his unease in October 2014 shortly after the announcements from Apple and Google:

> "Unfortunately, the law hasn't kept pace with technology, and this disconnect has created a significant public safety problem. We call it 'Going Dark,' and what it means is this: Those charged with protecting our people aren't always able to access the evidence we need to prosecute crime and prevent terrorism even with lawful authority. We have the legal authority to intercept and access communications and information pursuant to court order, but we often lack the technical ability to do so."[18]

In other public statements and Congressional testimony, Director Comey and others, including Deputy Attorney General Sally Yates, have continued to call attention to the problem. According to these statements, the going dark problem is being fueled by "the advent of default encryption settings and stronger encryption standards on both devices and networks,"[19] and, it may have a number of implications. For instance, according to FBI officials, "if there is no way to access the data . . . we may not be able to identify those who seek to steal our technology, our state secrets, our intellectual property, and our trade secrets."[20]

According to government officials, use of encryption may inhibit the ability of law enforcement and the intelligence community to investigate and prevent terrorist attacks. More specifically, Director Comey has stated that ISIS operators in Syria are "recruiting and tasking dozens of troubled Americans to kill people, [using] a process that increasingly takes part through mobile messaging apps that are end-to-end encrypted, communications that may not be intercepted, despite judicial orders under the Fourth Amendment."[21] FBI officials have also emphasized that the FBI does not possess the capability to defeat encryption using brute-force attacks and there is not an easy way to get around strong encryption.[22] Recently, Director Comey in Congressional testimony identified a terrorist attack in Garland, Texas, as an example: "[B]efore one of those terrorists left and tried to commit mass murder, he exchanged 109 messages with an overseas terrorist," Comey told a Senate committee. "We have no idea what he said, because those messages were encrypted."[23]

Others from the U.S. intelligence and law enforcement community, including NSA Director Admiral Michael Rogers, Homeland Security Secretary Jeh Johnson, and Attorney General Loretta Lynch have also voiced concerns about the going dark problem.[24] In the wake of the November 2015 ISIS-associated attacks in Paris, even in the absence of an on-the-record assertion that the terrorists used encryption to protect their communications, Central Intelligence Agency Director John Brennan suggested terrorists' use of technology "make it exceptionally difficult, both technically as well as legally, for intelligence and security services to have the insight they need to uncover it."[25] Whatever the assessment of the use of

encrypted communications to frustrate government investigations, a number of former officials from law enforcement and the intelligence community have disagreed about the need for a policy intervention.[26]

Although much of the debate in the media has focused on whether Director Comey is asking for companies like Google and Apple to preserve access to user data, no formal proposals have emerged from the FBI or other members of the law enforcement and intelligence communities. In July 2015, Director Comey noted in an appearance before the Senate Judiciary and House Intelligence Committees that "while there has not yet been a decision whether to seek legislation, we must work with Congress, industry academics, privacy groups, and others to craft an approach that addresses all of the multiple, competing legitimate concerns that have been the focus of so much debate in recent months."[27] Director Comey has also called on the private sector for help in identifying solutions that provide the public with security without frustrating lawful surveillance efforts. Most recently, in October 2015, Comey confirmed in testimony that the Obama administration will not, for the time being, pursue a legislative mandate, but will instead "continue conversations with industry" to find voluntary solutions.[28]

Similar debates are ongoing in other countries.[29] In the United Kingdom, Prime Minister David Cameron proposed an outright ban on end-to-end encryption technologies following the January 2015 attacks at the *Charlie Hebdo* offices in Paris.[30] The more recent November attacks in Paris have also caused French authorities to question policies surrounding the availability of encryption software.[31] Other European countries have passed or are considering legislation that would require companies to retain readable user data and provide access to government authorities on request.[32] And nation states that recognize fewer constitutional or other legal barriers to generating government demands for data, such as Saudi Arabia, Russia, and the U.A.E., have pioneered the use of pre-emptive legal mandates for data retention and decryption by technology providers.

Before we delve into the issues with the going dark metaphor, a few general observations are worth highlighting in brief.

The debate brings to the fore a number of tensions between security, privacy, economic competitiveness, and government access to information. A rich trove of expert literature explores these issues in detail.[33] Many of the technical and political merits of the debate were the focus of the recently published *Keys Under Doormats* report, authored by several of those who join this paper.[34] While these perspectives are out of scope for this paper, we acknowledge their importance for understanding the many dimensions of the going dark debate.

The global stage on which this debate is unfolding is worth emphasizing. Many geopolitical partners to the U.S. are actively engaged in discussions about promoting cybersecurity and the appropriate limits of surveillance across borders. For instance, the U.S.-E.U. Data Protection safe harbor, which provided a legal framework since the turn of the century for commercial cross-border data flows, was recently ruled invalid by the Court of Justice of the European Union due to concerns about the U.S. intelligence community's ability to access data.[35] The U.N. has also weighed in to a limited extent on encryption, recently declaring it "necessary for the exercise of the right to freedom of expression."[36]

Meanwhile, many U.S. companies must also answer to governments of foreign countries in which they do business. In this vein, they are increasingly playing a quasi-sovereign role as they face difficult decisions when foreign government agencies pressure them to produce data about citizens abroad. Many companies refuse to change the architecture of their services to allow such surveillance. However, if the U.S. government were to mandate architectural changes, surveillance would be made easier for both the U.S. government and foreign governments, including autocratic regimes known to crack down on political dissidents. The comparatively well-developed legal doctrines, procedural requirements, and redress mechanisms that serve as backstops to the U.S. government's surveillance activities are not mirrored worldwide.

On the subject of surveillance tools and techniques, much has changed over the past twenty years. The digital revolution has proven to be a boon for surveillance – it has become possible to track and learn about individuals at very granular level.[37] Although use of encryption may present a barrier to surveillance, it may not be impermeable. There are many ways to implement encryption incorrectly and other weaknesses beyond encryption that are exploitable.[38] For example, encryption does not prevent intrusions at the end points, which has increasingly become a technique used in law enforcement investigations.[39] Encryption typically does not protect metadata, such as e-mail addresses and mobile-device location information, that must remain in plaintext to serve a functional purpose. Data can also be leaked into unencrypted media, through cloud backups and syncing across multiple devices.[40]

Going Dark is the Wrong Metaphor

The going dark metaphor suggests that communications are becoming steadily out of reach – an aperture is closing, and once closed we are blind. This does not capture the current state and trajectory of technological development.

To be sure, encryption and provider-opaque services make surveillance more difficult in certain cases, but the landscape is far more variegated than the metaphor suggests. There are and will always be pockets of

dimness and some dark spots – communications channels resistant to surveillance – but this does not mean we are completely "going dark." Some areas are more illuminated now than in the past and others are brightening. Three trends in particular facilitate government access. First, many companies' business models rely on access to user data. Second, products are increasingly being offered as services, and architectures have become more centralized through cloud computing and data centers. A service, which entails an ongoing relationship between vendor and user, lends itself much more to monitoring and control than a product, where a technology is purchased once and then used without further vendor interaction. Finally, the Internet of Things promises a new frontier for networking objects, machines, and environments in ways that we just beginning to understand. When, say, a television has a microphone and a network connection, and is reprogrammable by its vendor, it could be used to listen in to one side of a telephone conversation taking place in its room – no matter how encrypted the telephone service itself might be. These forces are on a trajectory towards a future with more opportunities for surveillance.

In this section, we hope to elucidate this counter narrative. We do not suggest that the problem the FBI and others have identified is necessarily solved by the availability of other sources of data, nor do we conflate availability with the government's ability to gain access. Rather, we think that the forces opening new opportunities for government surveillance mean that, whatever the situation with iOS 8 encryption versus its predecessor, "going dark" does not aptly describe the long-term landscape for government surveillance. Any debate about surveillance capabilities today that will result in lasting policy should take into account these larger trends.

Encryption Runs Counter to the Business Interests of Many Companies

Current company business models discourage implementation of end-to-end encryption and other technological impediments to company, and therefore government, access.

For the past fifteen years, consumer-facing Internet companies have relied on advertising as their dominant business model. Ads are frequently used to subsidize free content and services. Internet companies more recently have been shifting towards data-driven advertising, and the technology that facilitates advertising delivery has become more reliant on user data for targeting ads based on demographics and behaviors. Companies seek to make behavioral assessments to match ads to individuals on the fly. Google products display advertising determined by behavioral patterns, search queries, and other signals collected by Google.[41] Similarly, Facebook claims it is capable of reaching narrow audiences in advertising campaigns with "89% accuracy" based on location, demographics, interests, and behaviors.[42] Yahoo products are also supported by advertising.[43] And, the list goes on.

To fuel this lucrative market, companies typically wish to have unencumbered access to user data – with privacy assured through either restricting dissemination of identifiable customer information outside the boundaries of the company (and of governments, should they lawfully request the data). Implementing end-to-end encryption by default for all, or even most, user data streams would conflict with the advertising model and presumably curtail revenues. Market trends so far reflect that companies have little incentive to veer from this model, making it unlikely that end-to-end encryption will become ubiquitous across applications and services. As a result, many Internet companies will continue to have the ability to respond to government orders to provide access to communications of users.

Cloud computing entails the movement of data and software to centralized locations operated by companies instead of under direct user custody. This technology, made possible by ubiquitous connectivity, enables businesses and individuals to extend their computing resources through the Internet at remote data centers, much like a utility service.[44] As a result, products are increasingly being offered as services, which in turn marks a shift away from traditional notions of ownership and control, and more towards centralized repositories of user data. Software and data no longer need to be installed and stored locally on an individual's computer – they can be delivered through a cloud service (e.g., Google Apps) or stored remotely in a cloud storage service (e.g., Dropbox) where they can be conveniently accessed from anywhere through a web browser or a smartphone app.[45] Webmail, social networking, word processing, and other common applications are now typically delivered as networked services.[46] These services deliver substantial benefits and convenience to both individuals and companies, and they are often provided free in ad-subsidized models or in economical pay-as-you-go arrangements.[47]

End-to-end encryption is currently impractical for companies who need to offer features in cloud services that require access to plaintext data. For example, Google offers a number of features in its web-based services that require access to plaintext data, including full text search of documents and files stored in the cloud. In order for such features to work, Google must have access to the plaintext. While Apple says that it encrypts communications end-to-end in some apps it develops, the encryption does not extend to all of its services. This includes, in particular, the iCloud backup service, which conveniently enables users to recover their data from Apple servers. iCloud is enabled by default on Apple devices. Although Apple does encrypt iCloud backups,[48] it holds the keys so that users who have lost everything are not left without recourse. So while the data may be protected from outside attackers, it is still capable of being decrypted by Apple.[49] Since Apple holds the keys, it can be compelled through legal process to produce user data that resides in iCloud.

There are a number of other reasons why a shift to encryption or other architectures would not appeal to businesses. Encryption schemes often add complexity to the user experience. Former Facebook Chief Security Officer Joe Sullivan observed that Facebook "has been able to deploy end-to-end encryption for a long time," but it has held back due to the added complexity and because "when end-to-end encryption is done right, it's hard for the average person to communicate."[50] Google has also reportedly held off on implementing device encryption by default on locked Android devices due to performance issues, despite its announcements that it would do so in 2014.[51] To date, the latest version of Android does not enable encryption by default.

Fragmentation in software ecosystems can also impede the degree to which new conventions and architectural changes – especially those that would enable user-to-user encryption across different devices and services – become widespread. In these ecosystems, multiple points of control may exist that influence the types of apps and operating system updates that eventually filter down to end users.

For example, in the Android ecosystem, smartphones are controlled by the wireless providers and handset manufacturers who create customized versions of the Android operating systems for the phones they sell. These companies have little incentive to update older phones to the latest versions of Android, because it would require them to invest resources into making the customized features compatible with newer versions of Android.[52] In fact, many older Android smartphones are never updated to newer OS versions. According to Google, as of this writing, approximately 32% of Android devices are running the latest Lollipop, which was released in November 2014.[53] In addition, although the next version of Android released by Google may contain apps that support end-to-end encryption, a manufacturer or wireless provider may modify the software to include its own suite of custom apps that do not support encryption. Some of these companies may have commercial interests in retaining access to plaintext communications.[54] A wide variety of third-party messaging applications are also available on Google Play, and end users can install and use them in place of the pre-installed messaging app that ships on their phones. In order for end-to-end encryption to work properly, both a sender's and receiver's messaging apps must be able to support it, and not all do. If the ecosystem is fragmented, encryption is that much less likely to become all encompassing.

The Internet of Things and Networked Sensors Open Uncharted Paths to Surveillance

A plethora of networked sensors are now embedded in everyday objects. These are prime mechanisms for surveillance: alternative vectors for information-gathering that could more than fill many of the gaps left behind by sources that have gone dark – so much so that they raise troubling questions about how exposed to eavesdropping the general public is poised to become. To paint an overall picture of going dark

based upon the fact that a number of widely used applications and products have introduced encryption by default risks obscuring this larger trend.

According to analysts and commentators representing the conventional wisdom, the Internet of Things (IoT) is the next revolution in computing. Expert observers have suggested that "the Internet of Things has the potential to fundamentally shift the way we interact with our surroundings," at work, at home, in retail environments, in cars, and on public streets.[55] The IoT market is forecast to grow into a multi-trillion dollar industry within the next ten years,[56] and according to a survey of experts, it will have "widespread and beneficial effects by 2025."[57] This will result in significant changes in how members of society interact with one another and the inanimate objects around them.[58]

Appliances and products ranging from televisions and toasters to bed sheets, light bulbs, cameras, toothbrushes, door locks, cars, watches and other wearables are being packed with sensors and wireless connectivity.[59] Numerous companies are developing platforms and products in these areas.[60] To name but a few, Phillips, GE, Amazon, Apple, Google, Microsoft, Tesla, Samsung, and Nike are all working on products with embedded IoT functionality, with sensors ranging from gyroscopes, accelerometers, magnetometers, proximity sensors, microphones, speakers, barometers, infrared sensors, fingerprint readers, and radio frequency antennae with the purpose of sensing, collecting, storing, and analyzing fine-grained information about their surrounding environments. These devices will all be connected to each other via the Internet, transmitting telemetry data to their respective vendors in the cloud for processing.[61]

The audio and video sensors on IoT devices will open up numerous avenues for government actors to demand access to real-time and recorded communications. A ten-year-old case involving an in-automobile concierge system provides an early indication of how this might play out. The system enables the company to remotely monitor and respond to a car's occupants through a variety of sensors and a cellular connection. At the touch of a button, a driver can speak to a representative who can provide directions or diagnose problems with the car. During the course of an investigation, the FBI sought to use the microphone in a car equipped with such a system to capture conversations taking place in the car's cabin between two alleged senior members of organized crime. In 2001, a federal court in Nevada issued *ex parte* orders that required the company to assist the FBI with the intercept. The company appealed, and though the Ninth Circuit disallowed the interception on other grounds, it left open the possibility of using in-car communication devices for surveillance provided the systems' safety features are not disabled in the process.[62] Such assistance might today be demanded from any company capable of recording conversations or other activity at a distance, whether through one's own smartphone, an Amazon Echo, a

baby monitor, an Internet-enabled security camera, or a futuristic "Elf on a Shelf" laden with networked audio and image sensors.[63]

In February 2015, stories surfaced that Samsung smart televisions were listening to conversations through an onboard microphone and relaying them back to Samsung to automatically discern whether owners were attempting to give instructions to the TV.[64] A statement published in Samsung's privacy policy instructed users to "be aware that if your spoken words include personal or other sensitive information, that information will be among the data captured and transmitted to a third party through your use of the Voice Recognition."[65]

Any given step of Samsung's process makes sense to offer the TV's features. Voice recognition is a computationally intensive task, and the processing capabilities of a modern television would be insufficient to make such a feature work. This is a common challenge for IoT devices that have limited processing power and limited battery capacity. The solution, in this case, was to utilize cloud infrastructure through a network connection to send the voice data to a remote server for processing and interpretations of that data back to the television as machine-actionable commands. Simple commands, such as "switch to channel 13," could be processed locally, but more complex ones, such as "show me a sci-fi movie like last week's, but not with Jane Fonda," would need to be sent to the cloud infrastructure – and in Samsung's case, to a third party, for processing.

Similarly, Google's Chrome browsing software supports voice commands using the onboard microphone in a laptop or desktop computer. The feature is activated when a user states the phrase "OK Google," and the resource intensive voice processing takes place on Google's remote servers.[66] Even children's toys are beginning to possess these features. In April 2015, Mattel introduced "Hello Barbie," an interactive doll capable of responsive speech, which is accomplished by recording children's interactions with the doll through a microphone, processing it in the cloud, and sending verbal responses through a speaker on the doll.[67] IP video cameras have also risen in popularity in the last several years. Devices like the Nest Cam record high resolution video with a wide-angle lens camera broadcast over the Internet to account holders.[68] Users can tune into the recording from Nest's website or through an app on their phone, and a camera will send an alert if it detects motion or an unusual noise. The Nest Cam can also exchange data and interact with other devices, such as Nest's thermostats and smoke detectors, which themselves contain sensors and microphones.

Law enforcement or intelligence agencies may start to seek orders compelling Samsung, Google, Mattel, Nest or vendors of other networked devices to push an update or flip a digital switch to intercept the ambient communications of a target. These are all real products now. If the Internet of Things has as

much impact as is predicted, the future will be even more laden with sensors that can be commandeered for law enforcement surveillance; and this is a world far apart from one in which opportunities for surveillance have gone dark. It is vital to appreciate these trends and to make thoughtful decisions about how pervasively open to surveillance we think our built environments should be – by home and foreign governments, and by the companies who offer the products that are transforming our personal spaces.

Concluding Thoughts

The debate over encryption raises difficult questions about security and privacy. From the national security perspective, we must consider whether providing access to encrypted communications to help prevent terrorism and investigate crime would also increase our vulnerability to cyber espionage and other threats, and whether nations that do not embrace the rule of law would be able to exploit the same access. At the same time, from a civil liberties perspective, we must consider whether preventing the government from gaining access to communications under circumstances that meet Fourth Amendment and statutory standards strike the right balance between privacy and security, particularly when terrorists and criminals seek to use encryption to evade government surveillance.

In examining these questions, our group focused on the trajectory of surveillance and technology. We concluded that the "going dark" metaphor does not fully describe the future of the government's capacity to access the communications of suspected terrorists and criminals. The increased availability of encryption technologies certainly impedes government surveillance under certain circumstances, and in this sense, the government is losing some surveillance opportunities. However, we concluded that the combination of technological developments and market forces is likely to fill some of these gaps and, more broadly, to ensure that the government will gain new opportunities to gather critical information from surveillance.

Looking forward, the prevalence of network sensors and the Internet of Things raises new and difficult questions about privacy over the long term. This means we should be thinking now about the responsibilities of companies building new technologies, and about new operational procedures and rules to help the law enforcement and intelligence communities navigate the thicket of issues that will surely accompany these trends.