HEARING: "GEOLOCATION TECHNOLOGY AND PRIVACY"
BEFORE THE HOUSE COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM
MARCH 2, 2016, RAYBURN HOUSE OFFICE BLDG. RM. 2154

WRITTEN SUBMISSION BY

PAUL J. LARKIN, JR.
SENIOR LEGAL RESEARCH FELLOW
THE HERITAGE FOUNDATION
214 MASSACHUSETTS AVE., NE
WASHINGTON, DC 20002-4999

HEARING: "GEOLOCATION TECHNOLOGY AND PRIVACY"
BEFORE THE HOUSE COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM
MARCH 2, 2016, RAYBURN HOUSE OFFICE BLDG. RM. 2154

WRITTEN SUBMISSION BY PAUL J. LARKIN, JR.
SENIOR LEGAL RESEARCH FELLOW, THE HERITAGE FOUNDATION

Mr. Chairman, Mr. Ranking Member, Members of the Committee:

My name is Paul J. Larkin, Jr. I currently am a Senior Legal Research Fellow at The Heritage Foundation. Most of my career has involved working in the criminal justice system in one capacity or another. For example, I worked at the Department of Justice in the Organized Crime and Racketeering Section of the Criminal Division and in the Office of the Solicitor General. I briefly was an Associate Independent Counsel under then-Independent Counsel Larry Thompson. I later was Counsel to the Senate Judiciary Committee when Senator Orrin Hatch was the Chairman. And I was a Special Agent-in-Charge with the Criminal Investigation Division of the Environmental Protection Agency. The views I express in this testimony are my own and should not be construed as representing any official position of The Heritage Foundation.

The questions of whether and, if so, how Congress should regulate the information-gathering abilities of new technologies presents important public policy issues.[1] The specific issue before the committee today—the use of geolocation technology to identify and track a person's whereabouts by locating his cell phone[2]—certainly is one of them.[3] There are more than 300 million cellphone subscribers in the United States,[4] and

---

[1] The literature on the relationship between new technologies (e.g., the Internet, modern tracking devices) and the Fourth Amendment, federal law, and privacy is large and continues to grow. *See, e.g.*, Jonathan Zittrain, *Searches and Seizures in a Networked World*, 119 HARV. L. REV. F. 83 (2006). Professor Orin Kerr, in particular, has been prolific scholar on the issues raised by the intersection of modern technology and the Fourth Amendment. *See, e.g.*, ORIN S. KERR, COMPUTER CRIME LAW (3d ed. 2012); Orin S. Kerr, *The Fourth Amendment and the Global Internet*, 67 STAN. L. REV. 285 (2015); Orin S. Kerr, *Foreword: Accounting for Technological Change*, 36 HARV. J.L. & PUB. POL'Y 403 (2013); Orin S. Kerr, *An Equilibrium-Adjustment Theory of the Fourth Amendment*, 125 HARV. L. REV. 476 (2011); Orin S. Kerr, *Applying the Fourth Amendment to the Internet: A General Approach*, 62 STAN. L. REV. 1005 (2010); Orin S. Kerr, Ex Ante *Regulation of Computer Search and Seizure*, 96 VA. L. REV. 1241 (2010); Orin S. Kerr, *Fourth Amendment Seizures of Computer Data*, 119 YALE L.J. 700 (2010); Orin S. Kerr, *Four Models of Fourth Amendment Protection*, 60 STAN. L. REV. 503 (2007); Orin S. Kerr, *Digital Evidence and the New Criminal Procedure*, 105 COLUM. L. REV. 279 (2005); Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531 (2005); Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801 (2004); *see also* Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 12085 (2004); Orin S. Kerr, *Internet Surveillance Law After the USA Patriot Act: The Big Brother That Isn't*, 97 NW. U. L. REV. 607 (2003).

[2] For a discussion of the technology and mechanics involved, see United States v. Graham, 796 F.3d 332, 343 (4th Cir.), *reh'g en banc granted*, 624 Fed. Appx. 75 (2015); Stephanie Lockwood, *Who Knows Where You've Been? Privacy Concerns Regarding the Use of Cellular Phones as Personal Locators*, 18 HARV. J.L. & TECH. 307, 308-10 (2004); Kevin McLaughlin, Note, *The Fourth Amendment and Cell Phone Location Tracking: Where are We?*, 29 HASTINGS COMM. & ENT. L.J. 421, 426-27 (2007).

[3] Various commentators have written on this subject. *See, e.g.*, Fabio Arcila, Jr., *GPS Tracking Out of Fourth Amendment Dead Ends:* United States v. Jones *and the* Katz *Conundrum*, 91 N.C. L. REV. 1 (2012);

law enforcement agencies submit massive number of requests for information to cell phone carriers each year.[5] The Baltimore Police Department alone has used a new, still largely secret technology to identify the location of cell phones 4,300 times since 2007.[6] It therefore is very important to law enforcement authorities and to the public at large whether and, if so, how the police may use the ability of cell phones to communicate their locations if the police need to locate the parties who own those phones.

For some time now, Congress has stepped in to regulate the government's use of information available through one new technology or another in order to balance law enforcement needs and privacy interests. Probably the two best-known examples are Title III of the Omnibus Crime Control and Safe Streets Act of 1968,[7] which regulates the use of wiretapping to obtain the content of spoken communications, and the USA PATRIOT Act of 2001,[8] which revised numerous federal electronic surveillance laws in response to the 9/11 attacks to enhance the nation's abilities to share relevant information between our intelligence and federal law enforcement agencies. There are several other laws on

---

Evan Bernick, *Protecting Americans' Privacy: Why the Electronic Communications Privacy Act Should Be Amended*, THE HERITAGE FOUNDATION, LEGAL MEMORANDUM No. 118 (Feb. 28, 2014), http://thf_media.s3.amazonaws.com/2014/pdf/LM118.pdf; Patrick T. Chamberlain, *Court Ordered Disclosure of Historical Cell Site Location Information: The Argument for a Probable Cause Standard*, 66 WASH. & LEE L. REV. 1745 (2009); William Curtiss, Note, *Triggering A Closer Review: Direct Acquisition of Cell Site Location Tracking Information and the Argument for Consistency Across Statutory Regimes*, 45 COLUM. J.L. & SOC. PROBS. 139 (2011); Susan Freiwald, *Cell Phone Location Data and the Fourth Amendment: A Question of Law, Not Fact*, 70 MD. L. REV. 681 (2011); Renée McDonald Hutchins, *Tied Up in Knotts? GPS Technology and the Fourth Amendment*, 55 UCLA L. REV. 409 (2007); Megan L. McKeown, *Whose Line Is It Anyway? Probable Cause and Historical Cell Site Data*, 90 NOTRE DAME L. REV. 2039 (2015); Hon. Brian L. Owsley, *The Fourth Amendment Implications of the Government's Use of Cell Tower Dumps in Its Electronic Surveillance*, 16 U. PA. J. CONST. L. 1 (2013); Jeremy H. Rothstein, Note, *Track Me Maybe: The Fourth Amendment and the Use of Cell Phone Tracking to Facilitate Arrest*, 81 FORDHAM L. REV. 489 (2012); Eric J. Struening, *Checked in: Decreasing Fourth Amendment Protection Against Real-Time Geolocation Surveillance*, 45 U. MEM. L. REV. 561 (2015); Alexandra D. Vesalga, Comment, *Location, Location, Location: Updating the Electronic Communications Privacy Act to Protect Geolocational Data*, 43 GOLDEN GATE U. L. REV. 459 (2013); Jacob T. Whitt, Note, *Cell Phones as an Eye of the Government:* In re Application of the United States for Historical Cell Site Data, 88 TUL. L. REV. 831 (2014).

[4] 317.44 million as of 2014. http://www.statista.com/statistics/186122/number-of-mobile-cellular-subscriptions-in-the-united-states-since-2000/.

[5] *See* Stephanie K. Pell & Christopher Soghoian, *A Lot More Than A Pen Register, and Less Than A Wiretap: What the Stingray Teaches Us About How Congress Should Approach the Reform of Law Enforcement Surveillance Authorities*, 16 YALE J. L. & TECH. 134, 152 (2014) ("wireless carriers receive tens of thousands of court orders requiring the disclosure of location data per year") (footnote omitted); *id*. 152 n.66 (citing a 2012 letter from Sprint stating that "[o]ver the past five years, Sprint has received . . . 196,434 court orders for location information.").

[6] Justin Fenton, *Baltimore Police used secret technology to track cellphones in thousands of cases*, BALTIMORE SUN (Apr. 9, 2015), http://www.baltimoresun.com/news/maryland/baltimore-city/bs-md-ci-stingray-case-20150408-story.html.

[7] Pub. L. 90-351, 82 Stat. 197 (codified at various sections of Titles 18 and 42 (2012)).

[8] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA PATRIOT Act) of 2001, Tit. II, Pub. L. No. 107-56, 115 Stat. 272 (2001) (codified at scattered sections of the U.S. Code).

those subjects as well.[9] Accordingly, there is nothing unusual in Congress deciding to become involved in the regulation of electronic information gathering technology by the government.

No particular bill is under discussion today, so I will address some general issues that would arise in connection with those issues and any potential federal legislation on those subjects. I would like to make three main points. First, current Supreme Court Fourth Amendment case law allows the government to acquire historical geolocational information without any showing of justification or need. It is possible that the Supreme Court could fundamentally change Fourth Amendment law, but it has not done so yet. Second, a new technology used by law enforcement permits a police officer to intercept outgoing cell phone's signals and thereby learn the phone's location without obtaining that information from a carrier. That technology, however, raises a serious Fourth Amendment issue because it operates only by capturing the signals from every cell phone in the device's operating radius, thereby effectively, albeit briefly, shutting off the ability of numerous cell phone users innocent of any crime to communicate with others. Third, any legislative solution would require Congress to draw arbitrary lines, but some arbitrary lines are worse than others. In that regard, I would like to offer some suggestions about lines that the committee should consider avoiding and drawing when deciding whether and how to regulate the government's acquisition and use of geolocational information.

I. THE FOURTH AMENDMENT AND THE GOVERNMENT'S ACQUISITION OF GEOLOCATIONAL INFORMATION FROM A TELECOMMUNICATIONS CARRIER

The Stored Communications Act provides that a judge "shall issue" an order directing a telecommunications carrier to release geolocational information to the government if it "offers specific and articulable facts showing that there are reasonable grounds to believe that the . . . records or other information sought[ ] are relevant and material to an ongoing criminal investigation."[10] Federal, state, and local law enforcement officers often invoke that authority to obtain information necessary to identify, locate, and apprehend a suspected offender. It doubtless has proved invaluable in a considerable number of cases.

The Supreme Court has not squarely decided whether the Fourth Amendment requires law enforcement officers to obtain a search warrant, based on probable cause, to acquire historical geolocational information from a cell phone company. Three federal courts of appeals—the Third, Fifth, and Eleventh Circuits—have held that the government may obtain that information from a carrier without obtaining a warrant or establish-

---

[9] *See*, *e.g.*, Communications Assistance for Law Enforcement Act of 1994, Pub. L. No. 103-414, 108 Stat. 4279 (codified, as amended, at 47 U.S.C. §§ 1001-1010 (2012)); Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified, as amended, at 18 U.S.C. § 2701 et seq. (2012)); Stored Communications Act (SCA), Pub. L. No. 99-508, 100 Stat. 1848 (codified, as amended, at 18 U.S.C. §§ 27201-2701 (2012); Video Privacy Protection Act of 1988, Pub. L. 100-618, § 2(a)(2), 102 Stat. 3195 (1988) (codified, as amended, at 18 U.S.C. § 2710 (2012)); Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, 92 Stat. 1783 (1978) (codified, as amended, at 50 U.S.C. ch. 36 (2012)); Privacy Act of 1974, Pub. L. 93-579, 88 Stat. 1896 (codified at 5 U.S.C. § 552a (2012)).

[10] 18 U.S.C. § 2703(d) (2012). The SCA was enacted as Title II of the Electronic Communications Privacy Act of 1986 (ECPA).

ing probable cause.[11] Settled Fourth Amendment law, known as the Third Party Doctrine,[12] strongly supports that conclusion. The rationale is that the government's acquisition of such information from a carrier does not infringe on the privacy of an individual because the sought-after information is contained in the carrier's business records, not in the subscriber's personal files. If the Supreme Court were to adhere to that longstanding doctrine, the Fourth Amendment would impose no requirement on the government's acquisition of historical geolocational information from a carrier because that conduct does not constitute a "search" for Fourth Amendment purposes.

Nonetheless, there is intellectual ferment regarding this aspect of Fourth Amendment law. Five Justices have signaled a willingness to reconsider at least some aspects of that settled doctrine. They could decide to endorse a different approach to questions like this one, an approach known as the Mosaic Theory.[13] That theory would treat the government's acquisition of this information as a "search" if it can help supply a larger, overall larger picture of a person's life, thereby forcing the government to establish probable cause before a neutral magistrate and obtain a search warrant (or establish an exception to the warrant requirement) to obtain geolocational information from a carrier.

It is impossible to know whether the Supreme Court will ultimately decide to fundamentally change Fourth Amendment law. Under current law, however, the government's practice does not violate that provision.

A. THE THIRD PARTY DOCTRINE

The Fourth Amendment bars the government from conducting an unreasonable "search" or "seizure."[14] Those are terms of description and limitation; government conduct that cannot be characterized as the one or the other is not subject to regulation under the Fourth Amendment.[15] A "search" requires the government to infringe upon some-

---

[11] *See* United States v. Davis, 785 F.3d 498 (11th Cir. 2015) (en banc) (holding that the Fourth Amendment protects individuals from retrieval of cell phone location information); *In re* U.S. for Historical Cell Site Data, 724 F.3d 600 (5th Cir. 2013) (holding that orders to obtain historical cell site information for specified cell phones at the points where the user places and terminates a call are not categorically unconstitutional); *In re* U.S. for an Order Directing a Provider of Elec. Commc'ns Serv. to Disclose Records to the Gov't, 620 F.3d 304 (3d Cir. 2010) (holding that the Stored Communications Act does not require the government to show probable cause to obtain a court order under 18 U.S.C. § 2703(d) for cell site information). Nonetheless, underneath the agreement among the federal circuits on the correct outcome of those cases is a fairly widespread disagreement as to the proper rule among the judges who considered those cases. The Fifth Circuit decided the *Davis* case by a 2-1 vote, and the en banc Eleventh Circuit split 8-3. In addition, a panel of the Fourth Circuit held that the government must obtain a search warrant to acquire geolocational records from a carrier, United States v. Graham, 796 F.3d 332, 343 (4th Cir. 2015), but the court of appeals granted rehearing en banc, United States v. Graham, 624 Fed. Appx. 75 (2015). Oral argument is tentatively scheduled for March 2016.

[12] *See* Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561 (2009).

[13] *See* Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311 (2012).

[14] The Fourth Amendment provides: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."

[15] *See, e.g.*, Maryland v. Macon, 472 U.S. 463, 468-69 (1985).

one's "reasonable expectation of privacy," while a "seizure" requires the government to materially interfere with a person's freedom of movement or his possessory interest in a "house, paper, or effect."[16] Viewing and recording the latitude and longitude coordinates collected by a cell tower is not a seizure of that information, because it deprives neither the subscriber nor his carrier of any freedom of movement or use of a cell phone,[17] so the only question is whether the acquisition and use of that information is a "search."

The Supreme Court has decided several cases involving the use of various types of modern-day electronic devices to obtain information, including a person's whereabouts.[18] None of those cases, however, dealt specifically with the acquisition from a cell phone carrier and later use of historical geolocational information. A few federal circuit courts of appeals have addressed this issue. While there is at present no conflict among the circuits on the legality of this issue, there has been considerable disagreement among the judges who have participated in the relevant cases. Nonetheless, the principles underlying closely analogous Supreme Court decisions permit the government to obtain that information without a search warrant or even a lesser showing of justification.

The principal decision in that regard is *Smith v. Maryland*.[19] In *Smith*, the telephone company, at the request of the police officers investigating a robbery and harassment of the victim by someone who claimed to have been the robber, installed a pen register device at its central office to capture the phone numbers called by Smith, who was the suspect in those crimes. Smith called the victim again, and, using information obtained from the phone company, the police obtained a search warrant for Smith's home, which turned up additional evidence of his crimes. He moved to exclude the evidence on the ground that the telephone company's installation of the pen register device at the behest of the police interfered with a reasonable expectation of privacy that Smith had in the content of his telecommunications. In an opinion by Justice Harry Blackmun, the Court rejected Smith's claim.

At the outset the Court noted that, because the pen register was installed on telephone company property at the company's central office, Smith could not claim "that his 'property' was invaded or that police intruded into a 'constitutionally protected area.'"[20] Moreover, because the pen register did not record the content of any of his conversations,

---

[16] *Id*. at 469.

[17] *See* Arizona v. Hicks, 480 U.S. 321, 324 (1987) ("[T]he mere recording of the serial numbers did not constitute a seizure. To be sure, that was the first step in a process by which respondent was eventually deprived of the stereo equipment. In and of itself, however, it did not "meaningfully interfere" with respondent's possessory interest in either the serial numbers or the equipment, and therefore did not amount to a seizure."); *Macon*, 472 U.S. at 468-69.

[18] *See, e.g.*, Riley v. California, 134 S. Ct. 2473 (2014) (search of a cell phone); United States v. Jones, 132 S. Ct. 945 (2012) (installation of a GPS tracking device on a person's car); Kyllo v. United States, 533 U.S. 27 (2001) (information obtained from a thermal imaging device); United States v. Karo, 468 U.S. 705 (1984) and United States v. Knotts, 460 U.S. 276 (1983) (installation of a beeper in a container of chemicals); Katz v. United States, 389 U.S. 347 (1967) (installation of a microphone on the outside of a phone booth).

[19] 442 U.S. 735 (1979).

[20] *Id*. at 741.

the Court reasoned, Smith's Fourth Amendment claim had to stand or fall on his argument that the installation and use of a pen register "constituted a 'search,'" which, in turn, necessarily rested on his submission that he had a legitimate expectation of privacy in the numbers he dialed on his phone.[21] The Court doubted that people actually have a legitimate expectation of privacy in the numbers they call, since people are aware that the phone company collects that information for billing purposes.[22] In any event, the Court added, a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties, like the phone company.[23]

In so ruling, the Court relied on its decision in *United States v. Miller*,[24] in which the Court had concluded that a bank depositor has no legitimate expectation of privacy in the financial information he voluntarily conveys to the bank.[25] As the Court had explained in *Miller* and reiterated in *Smith*, "[t]he Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed."[26]

Smith is but one example of the Third Party Doctrine. In several other cases, the Supreme Court has made it clear that a person has no legitimate expectation of privacy in information he voluntarily shares with third parties.[27] That is true even if the third party gives someone an assurance of confidentiality, the Court has noted, because we all must accept the risk of betrayal. "[T]he Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed."[28]

That principle traces its lineage to the longstanding practice of using police officers in an undercover capacity to identify offenders and collect evidence of their crimes. For decades the police have used undercover officers to infiltrate organized crime syndicates and ongoing drug trafficking operations, to perform activities that are likely to attract parties interested in selling or buying stolen articles, and in a variety of other ways. Undercover operations have proved to be a critical police practice for effective law enforcement in numerous cases that could not otherwise be adequately investigated.

---

[21] *Id*. at 742.

[22] *Id*. at 742-43.

[23] *Id*. at 743-44.

[24] 425 U.S. 435 (1976).

[25] *Id*. at 442-43.

[26] *Smith*, 442 U.S. at 744 (quoting *Miller*, 425 U.S. at 443).

[27] *See*, *e.g.*, *Miller*, 425 U.S., at 442–444; Couch v. United States, 409 U.S. 322, 335–336 (1973); United States v. White, 401 U.S. 745, 752 (1971) (plurality opinion); Hoffa v. United States, 385 U.S. 293 (1966); Lopez v. United States, 373 U.S. 427 (1963).

[28] *Smith*, 442 U.S. at 744 (internal punctuation omitted).

In the 1960s, the Warren Court upheld that practice even though it took advantage of the gullibility of some offenders and betrayed the confidence of the rest.[29] As the Supreme Court explained in 1966 in *Hoffa v. United States*,[30] "'The risk of being overheard by an eavesdropper or betrayed by an informer or deceived as to the identity of one with whom one deals is probably inherent in the conditions of human society. It is the kind of risk we necessarily assume whenever we speak.'"[31] Over the decades since its decision in the *Hoffa* case the Court has reconsidered and reaffirmed its Warren Court-era precedents.[32] It is firmly settled law that police undercover operations do not constitute a "search" or a "seizure." The Third Party Doctrines follows logically from the decisions approving that practice.

The result in *Smith* answers the question here. Each person voluntarily decides to carry a cell phone on his person—there is no law requiring anyone to carry a cell phone—and the average person knows that, given the technology that cell phones use to communicate, an active cell phone broadcasts its location to the nearest cell tower. Under those circumstances, the government does not commit a search whenever it acquires a person's historical locations from his cell phone carrier. The government's acquisition and use of geolocational information from a cell phone carrier is just another example of the Third Party Doctrine.

Nonetheless, there is an additional factor that complicates this problem. A new legal theory, the Mosaic Theory, could replace the Third Party Doctrine and establish new Fourth Amendment law by treating this practice, and perhaps many others, as a "search."

B. THE MOSAIC THEORY

The traditional Fourth Amendment analysis applied by the Supreme Court requires courts to examine a series of linked government actions on a step-by-step basis. The first step is to determine whether one action or another that led to the acquisition of evidence amounted to a search or seizure.[33] If none so qualify, the analysis is over, and the evidence may be admitted in the government's case-in-chief at trial. If one action (or more) does amount to a search or seizure, the next step is to ask whether that conduct is lawful—that is, whether the search or seizure was justified by probable cause or reasonable suspicion.[34] If it (or they) satisfied Fourth Amendment requirements, the analysis again is over, and the evidence may be admitted at trial. If one or more of those actions fails those requirements, the next step is to determine whether there is a causal connec-

---

[29] *See* Hoffa v. United States, 385 U.S. 293 (1966); Lopez v. United States, 373 U.S. 427 (1963).

[30] 385 U.S. 293 (1966).

[31] *Id*. at 465 (quoting Lopez v. United States, 373 U.S. 427, 450 (19063) (Brennan, J., dissenting)). As even Justice Brennan noted in his dissent in *Lopez*, "It is not an undue risk to ask persons to assume, for it does no more than compel them to use discretion in choosing their auditors, to make damaging disclosures only to persons whose character and motives may be trusted." 373 U.S. at 450 (1963) (Brennan, J., dissenting).

[32] *See* Illinois v. Perkins, 496 U.S. 292 (1990); United States v. White, 401 U.S. 745 (1971).

[33] *See, e.g.*, Maryland v. Macon, 472 U.S. 463 (1985).

[34] *See, e.g.*, Illinois v. Gates, 462 U.S. 213 (1983); Terry v. Ohio, 392 U.S. 1 (1968).

tion between them and the evidence. If there is no such connection[35] or (what is tantamount to the same conclusion) if the police would inevitably have discovered the evidence regardless of the illegality,[36] the analysis is over and the evidence may be admitted at trial. Finally, if there is a direct causal relationship, the question is whether a reasonable law enforcement officer would have known that his conduct violated the Fourth Amendment.[37] If not, the evidence is admissible. If, on the other hand, such an officer would have known that his conduct ran afoul of the Fourth Amendment—that is, if a police officer willfully violated the law—then the evidence must be suppressed. Courts must follow each step in that process before moving on to the next one. Moreover, the analysis does not permit a court to step back and evaluate the entire course of government conduct, as if it were a picture in a Rorschach Test, and decide whether the totality of the government's conduct was unlawful even though each step was justified.

Recently, however, several judges on the D.C. Circuit Court of Appeals, joined by perhaps five Justices of the Supreme Court, suggested that a different approach may be in order in the case of electronic surveillance. In *United States v. Jones*,[38] federal agents and local police officers, working together in a task force, placed a GPS tracking device on a suspect's car, monitored his movements for 28 days, and used that information to tie him to the drugs that were distributed by a group devoted to the sale of cocaine and crack. On appeal from his conviction, Jones argued that the installation of the GPS device violated the Fourth Amendment, requiring the exclusion of any data it reported. A panel of judges on D.C. Circuit agreed with Jones.[39]

Writing for the court, Judge Douglas Ginsburg concluded that settled Fourth Amendment law would allow the police to observe Jones as he drove on the open roads or city streets.[40] But Jones' case could not be decided so easily, Judge Ginsburg noted, because tracking Jones' car for 28 days was different in kind from watching his movements on any one particular day. As Judge Ginsburg put it, "no single journey reveals the habits and patterns that mark the distinction between a day in the life and a way of life, nor the departure from a routine that, like the dog that did not bark in the Sherlock Holmes story, may reveal even more."[41] The judge then adverted to cases in which private parties demand the disclosure of information that the government seeks to withhold on national security grounds. In those cases, the court noted, the government often argues that a court, when deciding whether to disclose the sought-after information, must

---

[35] *See, e.g.*, Murray v. United States, 487 U.S. 533 (1988).

[36] *See, e.g.*, Nix v. Williams, 467 U.S. 431 (1984).

[37] *See, e.g.*, United States v. Leon, 468 U.S. 897 (1984).

[38] 132 S. Ct. 945 (2012).

[39] United States v. Maynard, 615 F.3d 544 (D.C. Cir. 2010), *aff'd sub nom*. United States v. Jones, 132 S. Ct. 945 (2012).

[40] *See, e.g.*, United States v. Knotts, 460 U.S. 276, 281-82 (1983) ("A person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another. When [the defendant] traveled over the public streets, he voluntarily conveyed to anyone who wanted to look the fact that he was traveling over particular roads in a particular direction, the fact of whatever stops he made, and the fact of his final destination when he exited from public roads onto private property.").

[41] *Maynard*, 615 F.3d at 562.

consider the entire body of potentially relevant information, rather than one specific item taken out of context, because separate, individual pieces of information when combined could create a "mosaic" that enables someone to learn information damaging to the nation.[42] The same principle, the court concluded, should apply to searches like the one in Jones' case. "The whole of one's movements over the course of a month is not constructively exposed to the public because, like a rap sheet, that whole reveals far more than the individual movements it comprises."[43] The D.C. Circuit therefore set aside Jones' convicted and remanded his case to the district court.

The Supreme Court granted the government's certiorari petition and affirmed the D.C. Circuit's judgment, but on a narrower ground than the basis for the circuit court's ruling. All nine Justices believed that the government's conduct was unlawful, but only five Justices joined in the majority opinion written by the late Justice Antonin Scalia. The majority concluded that the government had committed a search by attaching the GPS device to Jones' vehicle and using at trial the evidence acquired by monitoring his whereabouts for the ensuing four weeks.[44] A vehicle is clearly an "effect" for purposes of the Fourth Amendment, the majority explained, and the attachment of the GPS device constituted a physical trespass on Jones' car.[45] Because the government had not preserved its argument that any search was justified,[46] the majority upheld the D.C. Circuit's judgment.

Five justices joined in one of two other opinions.[47] Justice Samuel Alito, joined by Justices Ruth Bader Ginsberg, Stephen Breyer, and Elena Kagan, wrote an opinion concurring in the judgment. Justice Alito found the common-law approach used by the majority to be an artificial way to examine a problem that could only have arisen in the twenty-first century. In his words, "Is it possible to imagine a case in which a constable secreted himself somewhere in a coach and remained there for a period of time in order to monitor the movements of the coach's owner?"[48] Rather, he would have asked whether the long-term monitoring of the movements of his vehicle violated Jones' reasonable ex-

---

[42] *Id*. at 562.

[43] *Id*. at 561-6 "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 churchgoer, 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." *Id*. at 562.

[44] United States v. Jones, 132 S. Ct. 945 (2012).

[45] *Id*. at 949-51.

[46] *Id*. at 954.

[47] Although five Justices joined the two separate opinions, they did not all join in one opinion and therefore did not establish a majority opinion for the Court. The opinion by Justice Scalia constituted the majority opinion.

[48] *Id*. at 958 (Alito, J., concurring in the judgment).

pectations of privacy,[49] the same methodology that the Court had consistently followed since its 1969 decision in *Katz v. United States*,[50] a case involving wiretapping. Aside from being inconsistent with *Katz*, the majority's analysis, according to Justice Alito, was flawed in a variety of ways.[51] He believed that the majority came to the correct result, just for the wrong reasons.

Justice Sonia Sotomayor, who joined the majority opinion, also wrote a separate concurring opinion. In that opinion, Justice Sotomayor agreed with the majority's conclusion that the case should be decided on the narrow ground that the government had committed a trespass,[52] but also expressed sympathy for Justice Alito's conclusion that a physical trespass is an unnecessary predicate in the case of electronic surveillance.[53] She added, however, that perhaps it was time to reconsider the Third Party Doctrine, in its entirety or at least in the case of electronic surveillance, because the doctrine no longer represents a reasonable way to look at information storage in the digital age.[54]

---

[49] *Id*. at 958 (Alito, J., concurring in the judgment).

[50] 389 U.S. 347 (1967).

[51] *Id*. at 961-62 (Alito, J., concurring in the judgment) (citations omitted; emphasis in original):

> First, the Court's reasoning largely disregards what is really important (the *use* of a GPS for the purpose of long-term tracking) and instead attaches great significance to something that most would view as relatively minor (attaching to the bottom of a car a small, light object that does not interfere in any way with the car's operation). Attaching such an object is generally regarded as so trivial that it does not provide a basis for recovery under modern tort law. . . .But under the Court's reasoning, this conduct may violate the Fourth Amendment. By contrast, if long-term monitoring can be accomplished without committing a technical trespass—suppose, for example, that the Federal Government required or persuaded auto manufacturers to include a GPS tracking device in every car—the Court's theory would provide no protection.
>
> Second, the Court's approach leads to incongruous results. If the police attach a GPS device to a car and use the device to follow the car for even a brief time, under the Court's theory, the Fourth Amendment applies. But if the police follow the same car for a much longer period using unmarked cars and aerial assistance, this tracking is not subject to any Fourth Amendment constraints.
>
> . . . . .
>
> Third, under the Court's theory, the coverage of the Fourth Amendment may vary from State to State. If the events at issue here had occurred in a community property State or a State that has adopted the Uniform Marital Property Act, respondent would likely be an owner of the vehicle, and it would not matter whether the GPS was installed before or after his wife turned over the keys. In non-community-property States, on the other hand, the registration of the vehicle in the name of respondent's wife would generally be regarded as presumptive evidence that she was the sole owner. . . .
>
> Fourth, the Court's reliance on the law of trespass will present particularly vexing problems in cases involving surveillance that is carried out by making electronic, as opposed to physical, contact with the item to be tracked.

[52] *Id*. at 954-55 (Sotomayor, J., concurring).

[53] *Id*. at 955-56 (Sotomayor, J., concurring).

[54] "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.. . . This approach is ill suited to

C. COMPARING THE TWO DOCTRINES

Pointing to the views of the five Justices who joined the opinions of Justices Alito and Sotomayor in *Jones*, various commentators have predicted that the Supreme Court will eventually adopt the Mosaic Theory to analyze electronic information gathering and surveillance. Although that outcome is possible, it would signal a material change in the Supreme Court's longstanding Fourth Amendment analysis. It would also have several adverse consequences.[55]

One such consequence is the elimination or crippling of the Third Party Doctrine. The Mosaic Theory leaves open numerous questions that the courts would need to grapple with over a lengthy period.[56] Answering those questions, moreover, would force the courts to undertake an arbitrary line-drawing exercise as they attempt to decide which observations are too long, too intrusive, or too fruitful.[57] The courts also would need to decide whether there are other relevant factors, such as the crime under investigation. (Are longer periods justified for drug trafficking than murder investigations because the former endure for longer period, or are longer periods justified for murder cases because murder is a more serious crime? What about traffickers suspected of having committed murder?) If so, surveillance law could vary from one law enforcement department to another given their different missions (Is halting the shipment of drugs more important than halting the shipment of stolen firearms?) and the different resources they can bring to bear (Can a five-person sheriff's department conduct a longer period of technology-

---

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, . . . 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 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." *Id*. at 957 (Sotomayor, J., concurring) (citations and internal punctuation omitted).

[55] *See* Kerr, 107 Mich. L. Rev. at 566-600.

[56] "Although the mosaic theory derives from an admirable goal, I believe it is a troubling approach that courts should reject. The mosaic theory should be repudiated for three reasons. First, the theory raises so many novel and puzzling new questions that it would be difficult, if not impossible, to administer effectively as technology changes. Second, the mosaic theory rests on a probabilistic conception of the reasonable expectation of privacy test that is ill suited to regulate the new technologies that the mosaic theory has been created to address. And third, the theory interferes with statutory protections that better regulate surveillance practices outside of the sequential approach." *Id*. at 346.

[57] Consider, for example, the difficulty of knowing exactly how to characterize observations of a suspect. "Modern technological tools such as GPS devices can be programmed to record at any interval. The ability to program surveillance tools greatly complicates legal standards based on time. To appreciate this, imagine the police use a GPS device that is programmed to turn on and record the location of the car for only one hour a day. The device is otherwise dormant. If the police monitor that device over twenty-eight days, does that count as twenty-eight days of monitoring? Or is that only twenty-eight hours of monitoring?" *Id*. at 333. For other difficulties posed by the Mosaic Theory, see *id*. at 328-53.

reliant surveillance than the FBI, because the latter has more than 14,000 special agents it can draw on?).

The continuous development of new technologies also would force the courts to be willing to upset settled expectations and stare decisis considerations by reconsidering their decisions every few years or so as new devices (iPhones) replace older ones (pagers). That outcome would unsettle Fourth Amendment and police practices on a regular basis.

Worsening the problem of ongoing disruption in the law is the delay between the advent of a new device and a court ruling on its legality. Years could pass.[58] If technology has moved on, the decision becomes of only historical interest, with no ongoing practical significance for privacy-protection purposes, but leaving in its wake a potentially large number of convictions that must be set aside.

The current, discrete step-by-step approach to Fourth Amendment analysis is not perfect—What human invention is?—but it does not morph into an entirely new approach with every new product put out by Microsoft, Google, or any other firm in the high-tech industries. There is something to be said for the proposition that the devil you know is better than the devil you don't.

Those results would occasion a fundamental change in the approach to Fourth Amendment doctrine in another way. For the last half-century, the Supreme Court has sought to craft easily understandable rules for law enforcement to follow, in the belief that a rule-oriented body of law would be clearer and easier for police officers to understand than one that asked simply whether their conduct was reasonable. Of course, a "rule of reason" does have something to say for itself. It would be consistent with the text of the Fourth Amendment—which demands that searches and seizures be "reasonable"—and it would be follow along with the Supreme Court's oft-stated proposition that "reasonableness" is the governing principle in all Fourth Amendment inquiries.[59] A general reasonableness approach would also avoid the need to draw new lines as advanced information-gathering technologies come on stream.

But it would accomplish those results at a loss of considerable clarity in Fourth Amendment doctrine as courts grapple with the task of deciding what is "reasonable." Under that approach, the identical law enforcement conduct could be reasonable or unreasonable depending on the facts and circumstances of each case, such as the crime involved and the risk to public safety if it goes unsolved.[60] Different lowers courts could

---

[58] For example, the FBI placed the GPS tracker on Jones' car in 2005, but the Supreme Court did not decide that the placement was a search until 2012. *Jones*, 132 S. Ct. at 945, 948.

[59] *See, e.g.*, Riley v. California, 134 S. Ct. 2473, 2482 (2014) ("As the text makes clear, "the ultimate touchstone of the Fourth Amendment is 'reasonableness.'") (citation omitted).

[60] *See, e.g.*, Brinegar v. United States, 338 U.S. 160, 183 (1949) (Jackson, J., dissenting) ("If we assume, for example, that a child is kidnapped and the officers throw a roadblock about the neighborhood and search every outgoing car, it would be a drastic and undiscriminating use of the search. The officers might be unable to show probable cause for searching any particular car. However, I should candidly strive hard to sustain such an action, executed fairly and in good faith, because it might be reasonable to subject travelers to that indignity if it was the only way to save a threatened life and detect a vicious crime. But I should

find identical conduct to be reasonable or not based on their individual judgments about the importance of particular crimes (Should kidnapping be treated the same as murder? Should drug trafficking be treated the same as murder if the suspects are senior members of a drug cartel known for violence?) or the difficulty that particular law enforcement officers will have in investigating them (Should there be one rule for the NYPD, which has more than thirty thousand police officers, and a different rule police department with far fewer officers?) The absence of clear rules defining "searches" and "seizures", as well as the different justifications for each one, does not assist law enforcement perform its job or guarantee individuals that the government will respect their privacy interests.

Finally, unraveling the Third Party Doctrine puts at risk law enforcement undercover operations, practices that the Supreme Court has upheld for more than 50 years. The rationale given in cases such as *Hoffa v. United States*,[61] *United States v. White*,[62] and *Illinois v. Perkins*[63] that were decided by the Warren, Burger, and Rehnquist Courts why undercover practices do not constitute a search, a seizure, or a coercive environment is that we assume the risk that information we share with others is no longer secret and may not remain private. Each person can choose to whom he discloses details of his life or business. In so doing, however, given the fact that people are not always trustworthy, we each take the risk of further disclosure, whether done accidentally or due to a betrayal. The Fourth Amendment does not protect us against the negligence or dishonesty of others; that is our burden.

The Mosaic Theory would undercut that principle by creating an exception for instances in which we disclose digital information, rather than physical records or spoken words, to telecommunications carriers, under the theory that we "need" cell phones despite their location-identifying features. Perhaps, the Supreme Court would draw a line distinguishing police undercover operations from their use of cell phone technology, but that line would be an arbitrary one, because the principles underlying the Court's approval of undercover operations logically gave rise to the Third Party Doctrine that the Mosaic Theory would erase.

Those issues, however, are ones that the Supreme Court may take up in a future case. At present, cases like *Smith* are still good law.

II. THE FOURTH AMENDMENT AND THE GOVERNMENT'S DIRECT INTERCEPTION OF GEOLOCATIONAL INFORMATION

A recent technological development may have changed the Fourth Amendment calculus, regardless of whether the Supreme Court adopts the Mosaic Theory. Technology now enables law enforcement officers to obviate the need to obtain geolocational information from a carrier for a particular individual. Instead, the government may purchase a commercially available device known as a "cell site simulator" that, by posing as

---

not strain to sustain such a roadblock and universal search to salvage a few bottles of bourbon and catch a bootlegger.").

[61] 385 U.S. 293 (1966).

[62] 401 U.S. 745 (1971).

[63] 496 U.S. 292 (1990).

a true cell tower, intercepts cell phone transmissions before they reach the carrier's own tower.[64] The simulator works as follows: When turned on, a cell phone sends a signal to the nearest cell tower in case there is an outgoing or incoming communication. As a person moves from one cell tower area to another the phone disconnects from the original tower and connects to the closest one available, changing as a person moves. These devices work by capturing the communications emitted by a cell phone en route to a telecommunications carrier before they can reach the closest available real tower. In essence, these devices pose as a carrier's cell tower and trick a cell phone into sending it the same geolocational information that the phone would transmit to one of the carrier's own towers.

The Supreme Court and the federal circuit courts have not yet addressed the government's acquisition of geolocation information via a cell tower simulator. In fact, few courts have analyzed the issue at all, in part due to the federal government's efforts to keep the existence of such a device secret.[65] Cases are now pending before different lower appellate courts challenging the use of such devices on the ground that, by precisely identifying a person's location, they enable law enforcement authorities to conduct a search without a warrant or probable cause.[66] None of those cases has yet been decided, and their outcome is uncertain.

There are several material differences between the government's acquisition of information by using a cell tower simulator and by obtaining information from a telecommunications carrier. First, a simulator enables the government to obtain real-time information indicating where a cell phone owner *is*, rather than historical information where

---

[64] *See, e.g.*, U.S. Dep't of Justice, Department of Justice Policy Guidance: Use of Cell-Site Simulator Technology (2015), http://www.justice.gov/opa/file/767321/download; William Curtis, *Triggering a Closer Review: Direct Acquisition of Cell Site Location Tracking Information and the Argument for Consistency Across Statutory Regimes*, 45 COLUM. J. L. & SOC. PROBS. 139 (2011); Stephen E. Henderson, *Real-Time and Historic Location Surveillance After United States v. Jones: An Administrable, Mildly Mosaic Approach*, 103 J. CRIM. L. & CRIMINOLOGY 803 (2013); Stephanie K. Pell & Christopher Soghoian, *Your Secret Stingray's No Secret Anymore: The Vanishing Government Monopoly over Cell Phone Surveillance and Its Impact on National Security and Consumer Privacy*, 28 HARV. J.L. & TECH. 1 (2014); Pell & Soghoian, 16 YALE J. L. & TECH. at 145-47; Spenser S. Hsu, *Constitutionality of StingRay use by D.C. police is challenged*, WASH. POST (Feb. 23, 2016), https://www.washingtonpost.com/local/public-safety/constitutionality-of-stingray-use-by-dc-police-is-challenged/2016/02/23/d197cb52-d9b2-11e5-81ae-7491b9b9e7df_story.html; Andrea Noble, *D.C. police use of secret cellphone tracking technology challenged in sex assault case*, WASH. TIMES (Feb. 23, 2016), http://www.washingtontimes.com/news/2016/feb/23/dc-police-use-of-secret-cellphone-tracking-technol/print/. These devices go by the names StingRay, Triggerfish, Kingfish, and Hailstorm. The devices can be installed in a vehicle, added to a drone, or carried by hand. *See* Pell & Soghoian, 16 YALE J. L. & TECH. at 145-47.

[65] *See* Fenton, *supra* note 6.

[66] *See* Jones v. United States, No. 15-CF-322 (D.C. Ct. App.); Maryland v. Andrews, Sept. Term 2015, No. 1496 (Md. Ct. Spec. App.); *see also In re* Application by the United States for an Order Relating to Telephones Used by [Suppressed] (N.D. Ill. Nov. 9, 2015) (setting conditions non the issuance of a search warrant for such a device); *see also In re* Application by the United States for an Order Relating to Telephones Used by [Suppressed] (N.D. Ill. Nov. 9, 2015) (Magistrate Judge Ian Johnston) (imposing conditions on the used of information acquired by use of cell tower simulators). The Wisconsin Supreme Court in *State v. Tate*, 849 N.W.2d 798 (2015), assumed that use of such a device was a search and found it reasonable because it was supported by probable cause and a warrant.

he *was*. That information can be extremely valuable in the case of a crime, like kidnapping, that remains in progress as long as the victim is alive and prevented from leaving the offender's custody. Second, a simulator captures a cell phone's outgoing signals that are necessary for it to make or receive calls. In the process, the simulator briefly but effectively disables or "quiets" the phone for the duration of time that it remains within the operating radius of the device.[67] Acquiring historical cell phone data from a carrier does not have that effect. Third, a simulator does not disable only the cell phone of the particular suspect within its reach; it disables *every* phone within that perimeter, even the phones possessed and used by parties who are entirely innocent of any crime. The number of parties who suffer a loss of cell phone use when a simulator is used in a rural area could be small, but that is not the case when a simulator is used in a densely populated urban area, such as the borough of Manhattan in New York City. Fourth, a simulator enables the government to avoid presenting any justification for its use to a neutral magistrate because no federal law regulates its use. The Department of Justice has issued a policy statement seeking to regulate the use of simulators by federal law enforcement officers and any allied state or local officers working as part of a task force or team. But the bulk of state and local officers are under no federal legal obligation to comply with the Justice Department's policy when they use such a device to investigate state crimes.

Given those differences, this question arises: Is it reasonable to treat the government's interception of telecommunications data by using a cell tower simulator in the same manner as its acquisition of this information from a telecommunications carrier pursuant to a court order. A strong argument can be made that the former is a more intrusive practice and should be subject to at least some degree of regulation.

To start with, it is important to recognize that the Third Party Doctrine has no bearing on the proper answer to that question. That doctrine rests on the proposition that the sought-after records belong to the *carrier*, *not* the *subscriber*, even though they contain information about or provided by the subscriber to the carrier. By intercepting a signal before it reaches the intended carrier, the company never acquires the data and never compiles it into its own business records. Accordingly, cases like the Supreme Court's decision in *Smith* are beside the point.

Moreover, regardless of the effect that a simulator has on a *subscriber's* desire to remain secluded,[68] whenever a simulator disables *all* cell phones within its working radius, the government has interfered with the liberty and property interests of people who are not the suspect of any crime. A cell phone is an "effect" protected by the Fourth

[67] It is unclear how long a disruption can last, what is the average length of a disruption, or, on average, how many cell phones are disrupted.

[68] That effect will differ depending on whether the simulator discloses only that someone is in a public area (*e.g.*, a highway) rather than in a protected area (*e.g.*, a home). Disclosure of the fact that someone is on a public highway, for example, is not a Fourth Amendment search, *see* United States v. Karo, 468 U.S. 705 (1984), but the electronically-aided disclosure where a person can be found in his home is a search, *see* United States v. Knotts, 460 U.S. 276 (1983). The relevant question is not, as some have argued, whether a simulator provides a more precise location of a cell owner than past cell tower records; it may. The pertinent question is whether that more precise location is within a protected area like a home, or an unprotected location, like a highway.

Amendment,[69] and the government's use of a device that disables a cell phone from being used to communicate is tantamount to the "seizure" of that phone for as long as the device is in operation.[70] In densely populated urban areas, the number of affected cell phones could be quite large. Even a temporary seizure of someone's cell phone must be justified by reasonable suspicion that a crime is afoot[71] or a comparable legitimate justification for the need to briefly separate a person from his property.[72]

III. A LEGISLATIVE SOLUTION MAY REQUIRE CONGRESS TO DRAW ARBITRARY LINES, BUT SOME ARBITRARY LINES ARE WORSE THAN OTHERS

A. IS NEW LEGISLATION NECESSARY?

Arguments can be made on both sides of the question whether Congress should consider additional legislation on these subjects. Some may argue in favor of waiting for the courts to gain additional familiarity with these practices before attempting to adopt a new set of rules by legislation. The courts have proved quite capable of resolving these issues based only on existing legislation and the Fourth Amendment so there is no need to bring their efforts to a halt through new acts of Congress. New legislation would only disrupt the common law-like decisionmaking process, the argument would conclude, that we have traditionally accepted as the best approach to resolve contested law enforcement police practices.

By contrast, the argument in favor of taking up these subjects now would go as follows: The Supreme Court has been willing to grant Congress considerable deference in legislating on topics like this one. For example, after the Court struck down the then-existing New York state wiretapping law in *Berger v. New York*,[73] some people feared that the Court would prohibit wiretapping altogether. Congress revised then-pending federal wiretap legislation in light of the *Berger* decision, and the Supreme Court has never found that law to be unconstitutional.[74] Moreover, the Court has recently made known its belief that legislatures can do a better job than courts when it comes to regulating the permissible use of new technologies for evidence-gathering purposes.[75] In fact,

---

[69] *See* Riley v. California, 134 S. Ct. 2473 (2014) (ruling that the Fourth Amendment regulates the government's search of a cell phone's contents).

[70] *See, e.g.*, Illinois v. McArthur, 531 U.S. 326 (2001) (barring a homeowner from entering his house while the police execute a search warrant is a "seizure"); United States v. Place, 462 U.S. 696 (1983) (ruling that the temporary seizure of a person's luggage for inspection must be justified by reasonable suspicion); United States v. Van Leeuwen, 397 U.S. 249 (1970) (treating the detention of a mailed package as a seizure, but finding it reasonable in that case).

[71] *See, e.g.*, Terry v. Ohio, 392 U.S. 1 (1968) (ruling that the temporary detention of a person for questioning must be justified by reasonable suspicion).

[72] *See, e.g.*, *McArthur*, 531 U.S. at 311-33 (concluding that the temporary exclusion of a person from his home must be justified); *supra* note 70.

[73] 388 U.S. 41 (1967).

[74] *See, e.g.*, Dalia v. United States, 441 U.S. 238 (1979); Scott v. United States, 436 U.S. 128 (1978); United States v. Donovan, 429 U.S. 413 (1977).

[75] *See* City of Ontario, Cal. v. Quon, 560 U.S. 746, 759 (2010) ("The Court must proceed with care when considering the whole concept of privacy expectations in communications made on electronic equipment owned by a government employer. The judiciary risks error by elaborating too fully on the Fourth Amend-

the Court has pleaded with Congress to "let this cup pass away" from them[76] by taking up the issue itself.[77] That factor would counsel in favor of readdressing the existing legislation governing geolocational information acquisition and use now, particularly in light of the use of the new simulation technologies.

Legislatures are better than courts at line-drawing, especially when there is no alternative to using an arbitrary line to define, for example, the time period within which law enforcement officers may pursue a certain practice without first obtaining judicial approval. For example, the police may detain a suspect for questioning if they have a reasonable suspicion that he has been or may be involved in criminal activity, a brief detention known in the argot of law enforcement as a *Terry* stop.[78] A *Terry* stop "must be temporary and last no longer than is necessary to effectuate the purpose of the stop,"[79] but there is no fixed time period under the Fourth Amendment past which law enforcement may detain someone. "Much as a bright line rule would be desirable, in evaluating whether an investigative detention is unreasonable," the Court has explained, "common sense and ordinary human experience must govern over rigid criteria."[80] Congress, however, could define a specific time limit—say, 30 minutes—on the lawfulness of a *Terry* stop (although few might find that to be a good idea). Just as Congress could define a bright-line rule limiting the length of *Terry* stops for federal law enforcement officers, Congress could fix a limit on the length of time that federal law enforcement officers may gather historical or real-time geolocational information from a telecommunications carrier or by using a simulator without obtaining judicial approval.

Law enforcement use of a cell phone simulator involves a more pressing issue than the acquisition of historical cell location data from a carrier. Federal law does not

---

ment implications of emerging technology before its role in society has become clear. . . . In *Katz* [v. United States, 389 U.S. 347, 353 (1967)], the Court relied on its own knowledge and experience to conclude that there is a reasonable expectation of privacy in a telephone booth. . . . It is not so clear that courts at present are on so sure a ground. Prudence counsels caution before the facts in the instant case are used to establish far-reaching premises that define the existence, and extent, of privacy expectations enjoyed by employees when using employer-provided communication devices.").

[76] *Matthew* 26:39.

[77] *See Jones*, 132 S. Ct. at 964 (Alito, J., concurring in the judgment) ("In circumstances involving dramatic technological change, the best solution to privacy concerns may be legislative. . . . 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.").

[78] *See, e.g.*, Terry v. Ohio, 392 U.S. 1 (1969).

[79] United States v. Sharpe, 470 U.S. 675, 684 (1985) (citation omitted).

[80] *Id*. at 685; *see also, e.g*., *id*. at 685 ("Obviously, if an investigative stop continues indefinitely, at some point it can no longer be justified as an investigative stop. But our cases impose no rigid time limitation on *Terry* stops. While it is clear that the brevity of the invasion of the individual's Fourth Amendment interests is an important factor in determining whether the seizure is so minimally intrusive as to be justifiable on reasonable suspicion, . . . we have emphasized the need to consider the law enforcement purposes to be served by the stop as well as the time reasonably needed to effectuate those purposes. . . . . We understand the desirability of providing law enforcement authorities with a clear rule to guide their conduct. Nevertheless, we question the wisdom of a rigid time limitation. Such a limit would undermine the equally important need to allow authorities to graduate their responses to the demands of any particular situation.") (citations and internal punctuation omitted).

expressly regulate that practice, and the Justice Department's policy does not govern the independent actions of state and local police officers. Supreme Court law indicates that the intentional disruption of cell phone use by entirely innocent parties must be justified by, at least, reasonable suspicion.[81]

B. WHAT SHOULD NEW LEGISLATION LOOK LIKE?

There are several different ways that Congress could regulate the acquisition and use of geolocational information from carriers via court orders or by using cell tower simulators. As a practical matter, it is impossible to do so without drawing arbitrary lines. Some arbitrary lines, however, are worse than others. The reason is that some lines might appear to be sensible, but on closer analysis turn out to be unreasonable.

1. UNREASONABLE ARBITRARY LINES

There are several potential regulatory approaches that would involve drawing arbitrary lines that are unreasonable. Congress should avoid pursuing those approaches.

Limiting Unrestricted Geolocational Information-Gathering Ability to Identified Law Enforcement Agencies: One possibility would be to limit the authority to obtain geolocational information or use simulators without any prior showing of need or justification to only certain particular domestic law enforcement agencies, such as the Federal Bureau of Investigation (FBI or Bureau) or the U.S. Secret Service. The argument would be that those agencies have a greater need to immediate access to geolocational information than any other law enforcement agency may have. The FBI is responsible not only for domestic federal law enforcement crimes such as kidnapping, but also for counterterrorism and counterespionage efforts, while the Secret Service is responsible for protecting the lives of the President and Vice-President, all of which are matters as to which time may be of the essence. This approach would give those two agencies the ability to have unlimited acquisition and use of geolocational information, while requiring every other agency to obtain a search warrant. The effect would be to wall off the Bureau and Secret Service from all other police agencies.

That approach, however, is not likely to work as planned. In the first place, no such wall is likely to stand forever. It would not be long before other federal law enforcement agencies—the Drug Enforcement Administration readily comes to mind—seek to be added to that category on the ground that, for example, narcotrafficking is as great a threat to the national security as the crimes investigated by the FBI and Secret Service. Having made one hole in the wall, Congress would be under pressure to make others, for agencies like U.S. Marshal's Service or the Bureau of Alcohol, Tobacco, Firearms, and Explosives, on the ground that they too deal with violent criminals. State and local police departments would also maintain that they pursue violent criminals as well, more, in fact, than the federal government does. Congress may not have the authority to generally make rape a federal crime,[82] but the states certainly do, and every one of them has done so. The states will argue that, considering the number of violent crimes that they must

[81] *See supra* note 70 (collecting cases).

[82] *See, e.g.*, United States v. Morrison, 529 U.S. 598 (2000).

investigate, they have a far greater need for unlimited access to geolocational information than federal law enforcement officers generally have.

An additional problem is that the Bureau and Secret Service work with other federal, state, and local law enforcement partners in formal task forces or on an informal basis. That raises the problem of deciding what geolocational information FBI and Secret Service agents can share with their law enforcement colleagues. In order for a task force or informal group of officers to work together effectively, each partner must be able to share information with others. It would make little sense to decide that FBI agents should have unlimited access to geolocational data when investigating a kidnapping, but the local police detectives working side-by-side with them should not.

Atop that, any effort to distinguish among state and local law enforcement agencies regarding immediate access to geolocational information—say, authorizing only the New York City Police Department and a few other similar departments to have the same access as the FBI and Secret Service—is likely doomed to fail. Kidnappings in Mayberry, North Carolina, are no less important than kidnappings in the borough of Queens, New York. Denying the detectives investigating a kidnapping in a small jurisdiction access to the same information under the same conditions available to their counterparts in a major metropolitan area does little to enhance privacy, but could do a great deal to impede an investigation. That would be particularly true if the two jurisdictions are working together on the same case.

The final reason why this approach would not work is realpolitik. Few Members of Congress outside of New York would be willing to say to their state and local police agencies (let alone to their constituents) that they are not as good or as trustworthy as the NYPD. The result is that, over time, Congress is very likely to add additional federal, state, and local law enforcement departments to the category of favored agencies, thereby undoing any effort to regulate the acquisition of geolocational information by limiting its automatic availability to a limited number of federal agencies with a unique and compelling need for it.

Limiting Unrestricted Geolocational Information-Gathering Ability to Identified Offenses: Another option is to limit the acquisition and use of this information to the investigation of certain identified crimes. For example, Congress could limit acquisition and use of geolocational information to violent crimes or terrorism offenses. Unfortunately, that approach likely would run aground due to several legal and practical problems with its implementation.

To start with, there is no federal crime of "terrorism" per se. Acts of terrorism can be prosecuted as murder, kidnapping, mayhem, assault, and so forth, but there is no general federal crime of murder, kidnapping, mayhem, or assault. The federal government can prosecute murder only if it occurs on federal property (*e.g.*, the Pentagon) or the victim is someone expressly identified in federal law (*e.g.*, a Member of Congress). Otherwise, murder is a state crime, punishable under a state's general "police power," a power that the federal government lacks.[83]

[83] *See, e.g.*, United States v. Morrison, 529 U.S. 598 (2000); United States v. Lopez, 514 U.S. 549 (1995).

Congress could attempt to limit use of a simulator to investigations involving a "crime of violence." But that limitation is also likely to come a cropper. In 2015, the Supreme Court concluded that the term "violent felony," a term defined by federal law to include any felony that "involves conduct that presents a serious potential risk of physical injury to another,"[84] was unconstitutionally vague.[85] Approaching this problem in that manner therefore may not move the ball downfield very far. Moreover, attempted violent crimes and conspiracies to commit violent crimes are not *themselves* violent crimes, but law enforcement officers may need cell location information in order to prevent such crimes from occurring. It makes little sense to force police officers to await the commission of a substantive crime of violence before they can obtain information that would have enabled them to stop an offender in his tracks.

Finally, no limitation is likely to remain exclusive for long. Consider the history of Congress's repeated additions to the offenses for which the government may use wiretapping as an investigative technique. What started out as a small list now approaches virtually every federal crime defined by the U.S. Code. The same outcome would occur here. Whenever the media splash a crime across the headlines or on TV, some Member of Congress will seek to add it to that list, and no Member of Congress is likely to be willing to incur the wrath of a colleague or the voting public by opposing an effort to enlarge it. It makes little sense to assume the contrary.

2. Reasonable Arbitrary Lines

There are at least three reasonable (albeit arbitrary) lines that Congress could draw. First, a statute could authorize federal, state, and local law enforcement authorities to obtain geolocational information whenever (a) they have a reasonable suspicion that a crime has occurred, is in progress, or is in the offing; (b) they have a reasonable belief that the information may be necessary for a legitimate intelligence or national security reason that may not be connected to the commission of a crime; or (c) they have a reasonable belief that the information is necessary for a legitimate non-law enforcement purpose, such as the need to find a lost child or to find someone who may be in distress on medical grounds or otherwise.[86] Second, a statute could impose a domestic search warrant requirement if, after a reasonable period of time has elapsed—say, three, seven, or ten days—the government still has a legitimate need for geolocational information for one of the above reasons. Third, a statute could permit the government to maintain, and to share with other law enforcement or intelligence agencies, whatever geolocational information it acquires but only in connection with the particular suspect(s) at issue. Information relating to other parties should be quickly destroyed.

---

[84] 18 U.S.C. § 924(e)(1) and (e)(2)(B) (2012).

[85] *See* Johnson v. United States, 135 S. Ct. 2551 (2015).

[86] Law enforcement officers may intervene to protect public safety even when no potential crime may be involved. *See*, *e.g*., Brigham City, Utah v. Stuart, 547 U.S. 398, 403 (2006) ("[L]aw enforcement officers may enter a home without a warrant to render emergency assistance to an injured occupant or to protect an occupant from imminent injury. . . . The role of a peace officer includes preventing violence and restoring order, not simply rendering first aid to casualties; an officer is not like a boxing (or hockey) referee, poised to stop a bout only if it becomes too one-sided.").

Those lines would balance law enforcement or intelligence needs against the public's reasonable expectations of privacy. A reasonable suspicion requirement would not burden law enforcement. The reasonable suspicion requirement first adopted in *Terry v. Ohio*[87] enables a police officer to draw on his training, experience, and common sense, applied to the totality of the circumstances, when deciding whether criminal activity is afoot.[88] The individual factors that comprise reasonable suspicion may each be entirely innocent when considered by themselves, but when considered together establish a reasonable belief that a crime was, is being, or may be committed.[89] Reasonable suspicion requires more than a "hunch" that someone is involved in crime, but it demands only "some minimal level of objective justification,"[90] an amount of evidence that is far less proof than what would be necessary to satisfy a probable cause requirement.[91]

---

[87] 392 U.S. 1 (1968).

[88] *See, e.g.*, United States v. Arvizu, 534 U.S. 266, 277 (2002) (the totality-of-the-circumstances approach "allows officers to draw on their own experience and specialized training to make inferences from and deductions about the cumulative information available to them that might well elude an untrained person") (citations and internal punctuation omitted); United States v. Cortez, 449 U.S. 411, 417-18 (1981) ("[T]he essence of all that has been written is that the totality of the circumstances—the whole picture—must be taken into account. Based upon that whole picture the detaining officers must have a particularized and objective basis for suspecting the particular person stopped of criminal activity. . . . The idea that an assessment of the whole picture must yield a particularized suspicion contains two elements, each of which must be present before a stop is permissible. First, the assessment must be based upon all the circumstances. The analysis proceeds with various objective observations, information from police reports, if such are available, and consideration of the modes or patterns of operation of certain kinds of lawbreakers. From these data, a trained officer draws inferences and makes deductions—inferences and deductions that might well elude an untrained person. . . . [T]he evidence thus collected must be seen and weighed not in terms of library analysis by scholars, but as understood by those versed in the field of law enforcement. The second element contained in the idea that an assessment of the whole picture must yield a particularized suspicion is the concept that the process just described must raise a suspicion that the particular individual being stopped is engaged in wrongdoing.") (citations omitted).

[89] *See, e.g.*, *Arvizu*, 534 U.S. at 277 ("A determination that reasonable suspicion exists, however, need not rule out the possibility of innocent conduct."); United States v. Sokolow, 490 U.S. 1, 9-10 (1989) ("Any one of these factors is not by itself proof of any illegal conduct and is quite consistent with innocent travel. But we think taken together they amount to reasonable suspicion. . . . We said in *Reid v. Georgia*, [448 U.S. 438, 441 (1980)], there could, of course, be circumstances in which wholly lawful conduct might justify the suspicion that criminal activity was afoot. . . . Indeed, *Terry* itself involved a series of acts, each of them perhaps innocent if viewed separately, but which taken together warranted further investigation. We noted in [*Illinois v. Gates*, 462 U.S. 213, 243–44 n.13 (1983)] that innocent behavior will frequently provide the basis for a showing of probable cause, and that in making a determination of probable cause the relevant inquiry is not whether particular conduct is innocent or guilty, but the degree of suspicion that attaches to particular types of noncriminal acts. That principle applies equally well to the reasonable suspicion inquiry.") (citations, footnotes, and internal punctuation omitted).

[90] *See, e.g.*, *Sokolow*, 490 U.S. at 7; INS v. Delgado, 466 U.S. 210, 217 (1984).

[91] *See, e.g.*, *Sokolow*, 490 U.S. at 7 ("The officer, of course, must be able to articulate something more than an inchoate and unparticularized suspicion or hunch. . . . The Fourth Amendment requires some minimal level of objective justification for making [a] stop. . . . That level of suspicion is considerably less than proof of wrongdoing by a preponderance of the evidence. We have held that probable cause means a fair probability that contraband or evidence of a crime will be found, and the level of suspicion required for a *Terry* stop is obviously less demanding than that for probable cause[.]") (citations and internal punctuation omitted). There also is no requirement that law enforcement officers undertake the least intrusive method of investigation. *See, e.g.*, *id.* at 10-11.

Proof that a reasonable suspicion standard will not disrupt law enforcement can be seen in the Justice Department policy on the use of cell tower simulators. The Department requires a federal agent to have probable cause before he may use such a device. It follows that a reasonable suspicion requirement will not disrupt investigations into criminal activity.

CONCLUSION

Geolocation technology, if appropriately used, can serve as a valuable law enforcement tool. But it raises serious constitutional questions as well as legitimate issues about the privacy of those people who are innocent of any crime but whose phone service would be disrupted and whose data would be captured. Congress may wish to consider establishing some reasonable rules of the road to address those issues.

Thank you for the opportunity to help you work through these issues.

APPENDIX A

The Heritage Foundation is a public policy, research, and educational organization recognized as exempt under section 501(c)(3) of the Internal Revenue Code. It is privately supported and receives no funds from any government at any level, nor does it perform any government or other contract work.

The Heritage Foundation is the most broadly supported think tank in the United States. During 2014, it had hundreds of thousands of individual, foundation, and corporate supporters representing every state in the U.S. Its 2014 income came from the following sources:

Individuals 75%

Foundations 12%

Corporations 3%

Program revenue and other income 10%

The top five corporate givers provided The Heritage Foundation with 2% of its 2014 income. The national accounting firm of RSM US, LLP, audits the Heritage Foundation's books annually.

Members of The Heritage Foundation staff testify as individuals discussing their own independent research. The views expressed are their own and do not reflect an institutional position for The Heritage Foundation or its board of trustees.

APPENDIX B

SHORT BIOGRAPHY

Paul J. Larkin, Jr., is a Senior Legal Research Fellow in the Center for Legal and Judicial Studies at The Heritage Foundation, where he directs its project to counter abuse of the criminal law, particularly at the federal level. Before joining Heritage in September 2011, Paul held various positions with the federal government and in the private sector. At the U.S. Justice Department, he served as an attorney in the Organized Crime and Racketeering Section of the Criminal Division and as an Assistant to the Solicitor General. He briefly was an Associate Independent Counsel under Independent Counsel Larry Thompson. Later, he was Counsel to the U.S. Senate Judiciary Committee and head of the Crime Unit for then-Chairman Senator Orrin Hatch. Afterwards, he was Special Agent-in-Charge for the Criminal Investigation Division of the Environmental Protection Agency, and briefly served as acting director in 2004. Paul received his undergraduate degree from Washington & Lee University; a law degree from Stanford Law School, where he was a published member of the Stanford Law Review; and a master's degree in public policy from George Washington University.