

From: (b)(6); (b)(7)(C)
Sent: 18 Sep 2019 18:55:28 +0000
To: (b)(6); (b)(7)(C)
Cc: Holz, Jordan; (b)(6); (b)(7)(C)
Subject: Venntel PTA DRAFT
Attachments: Venntel Gelocation Data Subscriptions (07 05 2019) DRAFT.docx

Hi (b)(6);
(b)(7)(C)

Please find attached the PTA Draft for Venntel. As discussed, the PTA is a preliminary draft and ICE Privacy will be making revisions once discussions on geolocation data have concluded. (b)(7)(E)

(b)(7)(E)

(b)(7)(E) Please feel free to reach out with any questions.

Thanks, (b)(6);
(b)(7)(C)

(b)(6); (b)(7)(C) **J.D./Joint M.S. Cybersecurity**
Management and Program Analyst
Office of Information Governance and Privacy, Privacy Division
U.S. Immigration and Customs Enforcement
Mobile: 401-826 (b)(6);
(b)(7)(C)
PCN: (b)(6);
(b)(7)(C)

Page 1424

Withheld pursuant to exemption

(b)(5) ; WIF Draft

of the Freedom of Information and Privacy Act

Page 1425

Withheld pursuant to exemption

(b)(5) ; WIF Draft

of the Freedom of Information and Privacy Act

Page 1426

Withheld pursuant to exemption

(b)(5) ; WIF Draft

of the Freedom of Information and Privacy Act

Page 1427

Withheld pursuant to exemption

(b)(5) ; WIF Draft

of the Freedom of Information and Privacy Act

Page 1428

Withheld pursuant to exemption

(b)(5) ; WIF Draft

of the Freedom of Information and Privacy Act

Page 1429

Withheld pursuant to exemption

(b)(5) ; WIF Draft

of the Freedom of Information and Privacy Act

Page 1430

Withheld pursuant to exemption

(b)(5) ; WIF Draft

of the Freedom of Information and Privacy Act

Page 1431

Withheld pursuant to exemption

(b)(5) ; WIF Draft

of the Freedom of Information and Privacy Act

Page 1432

Withheld pursuant to exemption

(b)(5) ; WIF Draft

of the Freedom of Information and Privacy Act

Page 1433

Withheld pursuant to exemption

(b)(5) ; WIF Draft

of the Freedom of Information and Privacy Act

Page 1434

Withheld pursuant to exemption

(b)(5) ; WIF Draft

of the Freedom of Information and Privacy Act

Page 1435

Withheld pursuant to exemption

(b)(5) ; WIF Draft

of the Freedom of Information and Privacy Act

Page 1436

Withheld pursuant to exemption

(b)(5) ; WIF Draft

of the Freedom of Information and Privacy Act

Page 1437

Withheld pursuant to exemption

(b)(5) ; WIF Draft

of the Freedom of Information and Privacy Act

Page 1438

Withheld pursuant to exemption

(b)(5) ; WIF Draft

of the Freedom of Information and Privacy Act

Page 1439

Withheld pursuant to exemption

(b)(5) ; WIF Draft

of the Freedom of Information and Privacy Act

Page 1440

Withheld pursuant to exemption

(b)(5) ; WIF Draft

of the Freedom of Information and Privacy Act

Page 1441

Withheld pursuant to exemption

(b)(5) ; WIF Draft

of the Freedom of Information and Privacy Act

From: (b)(6); (b)(7)(C)
Sent: 23 Oct 2019 19:56:41 +0000
To: (b)(6); (b)(7)(C)
Cc: Holz, Jordan (b)(6); (b)(7)(C)
Subject: Venntel - Geolocation Data Services Legal Review Process

Hi (b)(6);
(b)(7)(C)

(b)(6); (b)(7)(C); (b)(5)

Thanks (b)(6);
(b)(7)(C)

(b)(6); (b)(7)(C) **J.D./Joint M.S. Cybersecurity**
Management and Program Analyst
Office of Information Governance and Privacy, Privacy Division
U.S. Immigration and Customs Enforcement
Mobile: 401-826-(b)(6);
(b)(7)(C)
PCN: (b)(6);
(b)(7)(C)

From: (b)(6); (b)(7)(C)
Sent: 23 Oct 2019 20:37:52 +0000
To: (b)(6); (b)(7)(C)
Subject: Venntel

Hi (b)(6);
(b)(7)(C)

Hope all is well! Have you heard anything lately from DHS OGC on Venntel?

(b)(6); (b)(7)(C)
Associate Legal Advisor
Homeland Security Investigations Law Division
Office of the Principal Legal Advisor
U.S. Immigration and Customs Enforcement
202-732-(b)(6); (office)
202-494-(b)(7)(C) (mobile)
(b)(6); (b)(7)(C)@ice.dhs.gov

***** WARNING *** ATTORNEY/CLIENT PRIVILEGE *** ATTORNEY WORK PRODUCT *****

This document contains confidential and/or sensitive attorney/client privileged information or attorney work product and is not for release, review, retransmission, dissemination or use by anyone other than the intended recipient. Please notify the sender if this message has been misdirected and immediately destroy all originals and copies. Any disclosure of this document must be approved by the Office of the Principal Legal Advisor, U.S. Immigration & Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY. FOIA exempt under 5 U.S.C. § 552(b)(5).

From: (b)(6); (b)(7)(C)
Sent: 23 Oct 2019 20:33:10 +0000
To: (b)(6); (b)(7)(C)
Cc: Holz, Jordan (b)(6); (b)(7)(C)
Subject: RE: Venntel - Geolocation Data Services Legal Review Process

Hi (b)(6); (b)(7)(C)

(b)(6); (b)(7)(C); (b)(5)

(b)(6); (b)(7)(C)
Associate Legal Advisor
Homeland Security Investigations Law Division
Office of the Principal Legal Advisor
U.S. Immigration and Customs Enforcement
202-732 (b)(6); (b)(7)(C) (office)
202-494 (b)(6); (b)(7)(C) (mobile)
(b)(6); (b)(7)(C) @ice.dhs.gov

*** WARNING *** ATTORNEY/CLIENT PRIVILEGE *** ATTORNEY WORK PRODUCT ***

This document contains confidential and/or sensitive attorney/client privileged information or attorney work product and is not for release, review, retransmission, dissemination or use by anyone other than the intended recipient. Please notify the sender if this message has been misdirected and immediately destroy all originals and copies. Any disclosure of this document must be approved by the Office of the Principal Legal Advisor, U.S. Immigration & Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY. FOIA exempt under 5 U.S.C. § 552(b)(5).

From: (b)(6); (b)(7)(C) @ice.dhs.gov>
Sent: Wednesday, October 23, 2019 3:57 PM
To: (b)(6); (b)(7)(C) @ice.dhs.gov>
Cc: Holz, Jordan (b)(6); (b)(7)(C) @ice.dhs.gov>; (b)(6); (b)(7)(C) @ice.dhs.gov>
Subject: Venntel - Geolocation Data Services Legal Review Process

Hi (b)(6); (b)(7)(C)

(b)(6); (b)(7)(C); (b)(5)

Thanks, (b)(6); (b)(7)(C)

(b)(6); (b)(7)(C) J.D./Joint M.S. Cybersecurity
Management and Program Analyst
Office of Information Governance and Privacy, Privacy Division

U.S. Immigration and Customs Enforcement

Mobile: 401-826-(b)(6);
(b)(7)(C)

PCN: (b)(6);
(b)(7)(C)

From: (b)(6); (b)(7)(C)
Sent: 28 Oct 2019 19:25:09 +0000
To: (b)(6); (b)(7)(C)
Cc: Holz, Jordan (b)(6); (b)(7)(C)
Subject: RE: Venntel - Geolocation Data Services Legal Review Process

Thanks (b)(6); (b)(7)(C) I will keep you in the loop as well.

From: (b)(6); (b)(7)(C)@ice.dhs.gov>
Sent: Monday, October 28, 2019 2:43 PM
To: (b)(6); (b)(7)(C)@ice.dhs.gov>
Cc: Holz, Jordan (b)(6); (b)(7)(C)@ice.dhs.gov> (b)(6); (b)(7)(C)@ice.dhs.gov>
Subject: RE: Venntel - Geolocation Data Services Legal Review Process

Hi (b)(6); (b)(7)(C)

(b)(6); (b)(7)(C); (b)(5)

(b)(6); (b)(7)(C)

Associate Legal Advisor
Homeland Security Investigations Law Division
Office of the Principal Legal Advisor
U.S. Immigration and Customs Enforcement
202-732 (b)(6); (b)(7)(C) office)
202-494 (b)(6); (b)(7)(C) mobile)

(b)(6); (b)(7)(C)@ice.dhs.gov

***** WARNING *** ATTORNEY/CLIENT PRIVILEGE *** ATTORNEY WORK PRODUCT *****

This document contains confidential and/or sensitive attorney/client privileged information or attorney work product and is not for release, review, retransmission, dissemination or use by anyone other than the intended recipient. Please notify the sender if this message has been misdirected and immediately destroy all originals and copies. Any disclosure of this document must be approved by the Office of the Principal Legal Advisor, U.S. Immigration & Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY. FOIA exempt under 5 U.S.C. § 552(b)(5).

From: (b)(6); (b)(7)(C)@ice.dhs.gov>
Sent: Wednesday, October 23, 2019 3:57 PM
To: (b)(6); (b)(7)(C)@ice.dhs.gov>
Cc: Holz, Jordan (b)(6); (b)(7)(C)@ice.dhs.gov> (b)(6); (b)(7)(C)@ice.dhs.gov>
Subject: Venntel - Geolocation Data Services Legal Review Process

Hi (b)(6); (b)(7)(C)

(b)(6); (b)(7)(C); (b)(5)

Thanks, (b)(6);
(b)(7)(C)

(b)(6); (b)(7)(C)

J.D./Joint M.S. Cybersecurity

Management and Program Analyst

Office of Information Governance and Privacy, Privacy Division

U.S. Immigration and Customs Enforcement

Mobile: 401-826- (b)(6);
(b)(7)(C)

PCN: (b)(6);
(b)(7)(C)

DON'T BE EVIL: THE FOURTH AMENDMENT IN THE AGE OF GOOGLE, NATIONAL SECURITY, AND DIGITAL PAPERS AND EFFECTS

*Andrew William Bagley**

TABLE OF CONTENTS

TABLE OF CONTENTS	153
I.ABSTRACT	154
II.INTRODUCTION.....	154
III.INFORMATION FREE FLOW IN THE AGE OF THE INTERNET	159
A. The NSA Terrorist Surveillance Program and Unresolved Issues	159
B. Privacy and Fourth Amendment concerns in the age of Google	161
IV.STATUTORY PROTECTIONS FOR ONLINE DATA	167
V.“DIGITAL PAPERS” AND “EFFECTS”?	170
A. Expectation of Privacy	170
B. Third-party doctrine	173
VI.TERMS OF SERVICE: AN IMPLIED CONSENT?.....	178
VII.“DON’T BE EVIL” TO “CAN’T BE EVIL”	183
A. The need to restrain third party service providers	183
B. The State Action Doctrine	185
C. Post-Jackson and Rethinking the State Action Doctrine.....	187
VIII. CONCLUSION	190

* Andrew William Bagley, Alexander von Humboldt German Chancellor Fellow; J.D., University of Miami School of Law, 2009; M.A. Mass Communication, University of Florida, 2006; B.A. Political Science, University of Florida, 2005; B.S. Public Relations, University of Florida, 2005. I would like to thank Professor Mario Barnes for his invaluable help and feedback as I explored this topic and the Alexander von Humboldt Foundation for its generous support.

I. ABSTRACT

This Article offers an overview of current Fourth Amendment law in light of evolving concepts of papers and effects, expectations of privacy online, and the third party and state action doctrines. Scholars have addressed some of these issues individually, but this Article analyzes the legal issues that subsist in the wake of the NSA Terrorist Surveillance Program dilemma and during Congress' current push to update the Electronic Communications Privacy Act. Individuals are increasingly turning to third party technology companies such as Google to host their most private papers and effects, yet in doing so are subjecting themselves to non-negotiated Terms of Service and their information to the mercy of a corporate slogan.

Citizens are dependent on third party online service providers for their daily lives at the same time that these companies are becoming more intermingled with government agencies. However, current statutes are too antiquated to apply Fourth Amendment protections to today's digital papers and effects. Moreover, the existing third-party doctrine ignores the anonymity of email and media service providers in the cloud, and the state action doctrine has not adapted to restrain these entities from voluntarily divulging amounts of data more vast than that traditionally collected by state actors through normal investigative means. This article advocates the modification of current Fourth Amendment doctrine to adjust to an era in which private entities voluntarily share potentially private data with governmental entities.

II. INTRODUCTION

The federal government often has solicited cooperation, assistance, and information from large private-sector companies, particularly during the past decade, to pursue national security investigations.¹ However, these roles recently reversed when information giant Google chose to voluntarily provide data to the National Security Agency (NSA) in hopes of boosting its own security.² This incident made clear the pertinence of privacy and

¹ See Jon D. Michaels, *All the President's Spies: Private-Public Intelligence Partnerships in the War on Terror*, 96 CALIF. L. REV. 901, 910 (2008) (exposing the relationship between the government and telecommunication industries as a prime example).

² Ellen Nakashima, *Google to Enlist NSA to Help It Ward Off Cyberattacks*,

2011] The Fourth Amendment in the Age of Google 155

constitutional concerns left unresolved when immunity was granted to companies involved in the NSA's Terrorist Surveillance Program³ and their prevalence during the current expansion of public-private information sharing partnerships.⁴ Americans are turning increasingly to cloud computing solutions and the private sector to create, store, and publish their personal *papers and effects*.⁵ Simultaneously, governments around the world are pressuring communication providers to make content more easily accessible.⁶ Therefore, it is necessary to explore the application of the Fourth Amendment to the realities of a converged digital world and to ponder whether citizens would change their online behaviors if they expected the government to have unfettered access to their data.⁷

Private companies increasingly provide vital services to citizens, some for free and others for a fee.⁸ In doing so, third

WASH. POST, Feb. 4, 2010, <http://www.washingtonpost.com/wp-dyn/content/article/2010/02/03/AR2010020304057.html>. Google has also met on multiple occasions with members of the National Security Council. Byron Acohido, *Consumer Advocacy Group Calls for Hearing on Alleged Google Spying*, USA TODAY, July 20, 2010, <http://content.usatoday.com/communities/technologylive/post/2010/07/consumer-advocacy-group-calls-for-hearing-on-google-spying/1>.

³ See Zachary Keller, Note, *Big Brother's Little Helper's: Telecommunication Immunity and the FISA Amendment Act of 2008*, 70 OHIO ST. L.J. 1215, 1218-21, 1232-33 (2009) (stating that the FISA Amendment Act of 2008 granted immunity to telecommunication companies that assisted in the NSA's Terrorist Surveillance Program); Associated Press, *Bush Signs Bill on Government Wiretapping*, MSNBC.COM (July 10, 2008, 4:45 PM), <http://www.msnbc.msn.com/id/25622627/> [hereinafter *Bush Signs Bill on Government Wiretapping*] (describing the debate over the Act as "a battle that pitted privacy and civil liberties concerns over the desire to prevent terror attacks").

⁴ See Siobhan Gorman, *U.S. Plans Cyber Shield for Utilities, Companies*, WALL ST. J., July 8, 2010, <http://online.wsj.com/article/SB10001424052748704545004575352983850463108.html>. Private sector companies are now allowing the NSA to install network monitoring sensors to protect critical infrastructure. *Id.*

⁵ See JANNA QUITNEY ANDERSON & LEE RAINIE, PEW RESEARCH CTR., *THE FUTURE OF CLOUD COMPUTING 2* (2010), available at http://pewinternet.org/~media/Files/Reports/2010/PIP_Future_of_the_Internet_cloud_computing.pdf.

⁶ Miguel Helft et al., *For Data, Tug Grows Over Privacy vs. Security*, N.Y. TIMES, Aug. 3, 2010, <http://query.nytimes.com/gst/fullpage.html?res=9504E4D6113CF930A3575BC0A9669D8B63&sec=&spon=&pagewanted=1>

⁷ Google's own CEO predicts that some people would change their names if the rest of the world had access to their online footprints. Murray Wardrop, *Young Will Have to Change Names to Escape 'Cyber Past' Warns Google's Eric Schmidt*, TELEGRAPH, Aug. 18, 2010, <http://www.telegraph.co.uk/technology/google/7951269/Young-will-have-to-change-names-to-escape-cyber-past-warns-Google-Eric-Schmidt.html>.

⁸ See, e.g., *Sample Bill*, AT&T, <https://www.customerservice.att.com>

parties such as information service provider, Google, and telecommunication giant, AT&T, amass large amounts of personal user data.⁹ In many instances, citizens relinquish personal data in exchange for free services, such as email and instant messaging, or low-cost long distance phone calls.¹⁰ Traditionally, such data has been used by companies for niche marketing and research purposes.¹¹ However, in recent years the United States government has built national security databases with personal user data allegedly obtained from cooperating telecommunication companies such as Bellsouth,¹² AT&T¹³ and Verizon.¹⁴

In 2006, lawsuits against Bellsouth, AT&T and Verizon alleged that the companies violated consumer confidentiality by

/sample_bills/sample_print_1ld.html (last visited Nov. 29, 2010) (AT&T provides phone services for a fee); *Welcome to Gmail*, GMAIL, <http://mail.google.com/mail/help/open.html> (last visited Nov. 29, 2010) (Google provides email service for free). An enormous population is transmitting their personal data through computer servers owned by private parties. See Solarina Ho, *Poll Finds Nearly 80 Percent of U.S. Adults Go Online*, REUTERS (Nov. 5, 2007, 8:35 PM), <http://www.reuters.com/article/internetNews/idUSN0559828420071106?feedType=RSS&feedName=internetNews&rpc=22&sp=true> (nearly 80% of American adults use the Internet).

⁹ See Elinor Mills, *Google Balances Privacy, Reach*, CNET NEWS (July 14, 2005, 4:00 AM), http://news.cnet.com/Google-balances-privacy-reach/2100-1032_3-5787483.html; Eric Benderoff & Jon Van, *Privacy? What Privacy?*, CHI. TRIB., May 14, 2006, http://articles.chicagotribune.com/2006-05-14/news/0605140367_1_google-privacy-digital.

¹⁰ See Robert Luke, *Web Portals as Purchasing Ideology*, 8 TOPIA: CAN. J. OF CULTURAL STUD. 61, 61, 64, 70–71, 71 n.11 (2002), available at <http://pi.library.yorku.ca/ojs/index.php/topia/article/viewFile/142/133> (explaining that to use ISP services such as email and instant messaging “clients must relinquish their personal data”); *Teach Your Phone New Tricks*, GOOGLE VOICE, <https://www.google.com/accounts/ServiceLogin?service=grandcentral&passive=1209600&continue=https://www.google.com/voice&followup=https://www.google.com/voice<mpl=open> (last visited Nov. 29, 2010) (showing that by creating a Google account, users can access Google Voice which provides free calls to the U.S. and Canada and provides “[s]uper low rates everywhere else”).

¹¹ Simon Lazarus & Brett Kappel, *Europeans Spur U.S. Debate: Protecting Privacy From Prying Eyes*, LEGAL TIMES, June 15, 1998.

¹² Cheryl Bronson & Pam Benson, *BellSouth, AT&T Added to NSA Lawsuit*, CNN.COM (May 17, 2006), <http://edition.cnn.com/2006/POLITICS/05/16/NSA.suit/>.

¹³ Leslie Cauley, *NSA Has Massive Database of Americans' Phone Calls*, USA TODAY, May 11, 2006, http://www.usatoday.com/news/washington/2006-05-10-nsa_x.htm.

¹⁴ Marguerite Reardon, *Verizon Sued for Alleged NSA Cooperation*, CNET NEWS (May 15, 2006, 3:16 PM), http://news.cnet.com/Verizon-sued-for-alleged-NSA-cooperation/2100-1036_3-6072483.html.

2011] The Fourth Amendment in the Age of Google 157

partnering with the National Security Agency (NSA) to monitor phone calls and turn over phone records.¹⁵ Although the lawsuits eventually were mooted by legislation,¹⁶ larger constitutional questions emerged.¹⁷ The U.S. government did not obtain warrants to monitor the phone calls, nor did it rely upon subpoenas to obtain user information as part of the wiretapping program.¹⁸ Thus, the traditional legal process was evaded, and the government obtained potentially incriminating information through voluntary agreements with private corporations.¹⁹ The Fourth Amendment likely was not triggered because private companies did the data gathering and managed the phone calls; therefore, no explicit state action was present.²⁰ The companies waived their own Fourth Amendment rights by consenting to the government's requests and did not necessitate the government's use of the subpoena or warrant process.

Modern citizen behavior makes it important to reexamine aspects of the third party and state action doctrines in light of blurring private-public boundaries and customer-citizen distinctions. For purposes of illustrating the epitome of private-

¹⁵ *Terkel v. AT&T Corp.*, 441 F. Supp. 2d 899, 900, 911 (N.D. Ill. 2006); *Hepting v. AT&T Corp.*, 439 F. Supp. 2d 974, 978, 988 (N.D. Cal. 2006); *In re Nat'l Sec. Agency Telcomms. Records Litig.*, 444 F. Supp. 2d 1332, 1333-34 (J.P.M.L. 2006).

¹⁶ See *Bush Signs Bill on Government Wiretapping*, *supra* note 3 (describing the bill signed into law by President Bush to grant immunity to telecommunications companies that helped the U.S. government "spy on Americans in suspected terrorist cases").

¹⁷ See David Kravets, *Courts, Congress Shun Addressing Legality of Warrantless Eavesdropping*, WIRED.COM (Jan. 29, 2010, 4:00 PM), <http://www.wired.com/threatlevel/2010/01/legality-of-warrantless-eavesdropping/> (noting that AT&T's alleged "funneling . . . of its customers' electronic communications to the [NSA] – without warrants" precipitated a lawsuit claiming "major violations of the Fourth Amendment right to be free from warrantless searches and seizures").

¹⁸ Reardon, *supra* note 14; *Verizon Sued over NSA Surveillance*, SPAM DAILY NEWS (May 13, 2006), http://www.spamdailynews.com/publish/Verizon_sued_over_NSA_surveillance.shtml; David Kravets, *Judge Tosses Telecom Spy Suits*, WIRED.COM (June 3, 2009, 2:30 PM), http://www.wired.com/threatlevel/2009/06/telecom_suit/.

¹⁹ See Cauley, *supra* note 13.

²⁰ The state action doctrine allows for liabilities to attach to government actors for private actions in certain circumstances. *Villegas v. Gilroy Garlic Festival Ass'n*, 541 F.3d 950, 954–55 (9th Cir. 2008) ("[S]tate action may be found if, though only if, there is such a 'close nexus between the State and the challenged action' that seemingly private behavior 'may be fairly treated as that of the States itself.'" (quoting *Brentwood Acad. v. Tenn. Secondary Sch. Athletic Ass'n*, 531 U.S. 288, 295 (2001))). However, such circumstances were not present here.

sector data collection, this research focuses on the evolution of *papers and effects* increasingly stored by third party Internet giants such as Google. Congress is currently holding hearings to update the Electronic Communications Privacy Act which provides the bulk of statutory protection for email privacy.²¹ However, this article argues that statutory protections alone are inadequate to protect the evolving concept of a person's papers and effects and that Fourth Amendment jurisprudence must adapt to modern digital trends. Moreover, these legal issues must be resolved so that the government and third party service providers alike can unambiguously comply with constitutional requirements while cooperating.²² Part I of this article provides an overview of the current Internet age privacy dilemma. Part II identifies current statutory protections afforded to online data and exposes ambiguous and unprotected areas.

Part III explains how the *papers and effects* protected by the Fourth Amendment are increasingly migrating into the digital domain and identifies the extent of a reasonable expectation of privacy in an online world controlled by third parties. Part IV discusses the prospect of implicit consumer consent to searches via contracts of adhesion. Part V highlights the state action doctrine and addresses the possibility of applying it to prevent another NSA dragnet debacle. Lastly, the conclusion advocates the recognition of full Fourth Amendment protections for digital papers and effects to adequately address the realities of the privacy and national security roles played by private actors.

²¹ See Gabriel Perna, *Congress Eyes Reform of Wiretapping Law*, INT'L BUS. TIMES, (June 25, 2010, 2:59 AM), <http://uk.ibtimes.com/articles/30636/20100624/congress-eyes-reform-of-wiretapping-law.htm>.

²² A whole coalition of communication providers supports reforming the ECPA to update privacy laws to match the realities of consumer behavior. See Sam Gustin, *Google, Microsoft, ACLU Form 'Digital Due Process' for E-Privacy Reform*, DAILY FIN. (Mar. 30, 2010, 3:40 PM), <http://www.dailyfinance.com/story/company-news/google-microsoft-aclu-form-digital-due-process-for-e-privacy/19420228/>. This coalition includes companies such as Google and Microsoft who provide cloud computing services and even AT&T which participated in the NSA Terrorist Surveillance Program. See *id.*; *About the Issue*, DIGITAL DUE PROCESS, <http://www.digitaldueprocess.org> (last visited Nov. 29, 2010).

2011] **The Fourth Amendment in the Age of Google** 159

III. INFORMATION FREE FLOW IN THE AGE OF THE INTERNET

A. The NSA Terrorist Surveillance Program and Unresolved Issues

The Bush administration authorized a large scale electronic communications interception program after the attacks of September 11, 2001 dubbed the Terrorist Surveillance Program (TSP).²³ While the aim of the program was to intercept evidence in order to prevent terrorist attacks, the lack of court authorization by way of subpoena or warrant raised the prospect of government fishing expeditions.²⁴ Moreover, questions emerged challenging whether or not the administration violated the Foreign Intelligence Surveillance Act which governs surreptitious domestic intelligence gathering. The Electronic Frontier Foundation alleged that the telephone companies allowed the government to utilize their networks to capture telephone, e-mail, and web browsing activities of millions of people.²⁵

Companies such as AT&T claimed that they merely complied with government requests for national security purposes that were lawful under the Wiretap Act,²⁶ which permits the Attorney General to certify that communications may lawfully be intercepted without a warrant.²⁷ Wholly domestic phone calls and data were monitored by the NSA in at least some instances, despite initial government claims that the TSP merely monitored calls where at least one party was abroad.²⁸ Moreover, the NSA engaged in “significant and systemic” overuse of unwarranted, non-FISA interception of e-mails and phone calls well into 2009

²³ John Diamond & David Jackson, *Surveillance Program Protects Country, Bush Says*, USA TODAY, Jan. 23, 2006, http://www.usatoday.com/news/washington/2006-01-23-bush_x.htm.

²⁴ Mark Hosenball, *Hold the Phone*, NEWSWEEK (May 22, 2006), <http://www.newsweek.com/2006/05/21/hold-the-phone.html#>.

²⁵ Declan McCullagh, *Legal Loophole Emerges in NSA Spy Program*, CNET NEWS (May 17, 2006, 5:15 PM), http://www.news.com/Legal-loophole-emerges-in-NSA-spy-program/2100-1028_3-6073600.html?tag=nefd.lede [hereinafter *Legal Loophole Emerges in NSA Spy Program*].

²⁶ 18 U.S.C. § 2511 (2010).

²⁷ *Legal Loophole Emerges in NSA Spy Program*, *supra* note 25.

²⁸ James Risen & Eric Lichtblau, *Spying Program Snared U.S. Calls*, N.Y. TIMES, Dec. 21, 2005, <http://www.nytimes.com/2005/12/21/politics/2lnsa.html?ex=1292821200&en=91d434311b0a7ddc&ei=5088&partnpa=rssnyt&emc=rss>.

that exceeded limits imposed by Congress.²⁹

Two lawsuits filed against telecommunication companies in 2006 initially were permitted to continue on their merits despite the government's invocation of the state secrets doctrine. However the cases effectively were mooted by the FISA Amendments Act of 2008.³⁰ In *Hepting v. AT&T Corp.*, the District Court for the Northern District of California initially held that the state secrets privilege could not be used to dismiss a lawsuit against AT&T for its alleged involvement in the TSP because plaintiffs could proceed on other well known information about AT&T's collusion with the government.³¹ However, the case later was remanded to the district court, consistent with the immunity granted in the act.³² In *Al-Haramain Islamic Found., Inc. v. Bush*, the U.S. Court of Appeals for the Ninth Circuit held that the state secrets privilege could not be used to dismiss a TSP lawsuit against the government in which public knowledge existed about the contents of a classified document.³³ However, the case never was decided on its merits, and litigation is still pending with a group of other TSP lawsuits that challenge the constitutionality of the immunity clause in the FISA amendments.³⁴

The legal issues left unresolved by the thwarted TSP lawsuits are dwarfed by the prospect of larger data gathering schemes involving online service providers. The government's unwarranted seizure of phone data, while alarming, likely was insufficient to obtain convictions without further evidence.³⁵

²⁹ Eric Lichtblau & James Risen, *Officials Say U.S. Wiretaps Exceeded Law*, N.Y. TIMES, Apr. 15, 2009, http://www.nytimes.com/2009/04/16/us/16nsa.html?_r=3.

³⁰ See Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008, Pub. L. No. 110-261, 122 Stat. 2467-69, 2471 (2008) (granting electronic communication service providers immunity from suit for assisting the government pursuant to a directive from the Attorney General and the Director of National Intelligence).

³¹ *Hepting v. AT&T Corp.*, 439 F. Supp. 2d 974, 993-94, 1011 (N.D. Cal. 2006), *remanded by* 539 F.3d 1157 (9th Cir. 2008).

³² *Hepting v. AT&T Corp.*, 539 F.3d 1157, 1158 (9th Cir. 2008).

³³ *Al-Haramain Islamic Found., Inc. v. Bush*, 507 F.3d 1190, 1195-96, 1198, 1203-06 (9th Cir. 2007).

³⁴ See *In re Nat'l Sec. Agency Telecomms. Records Litig.*, 700 F. Supp. 2d 1182, 1185-92, 1197, 1203-04 (N.D. Cal. 2010).

³⁵ However, criminal convictions were obtained based on phone data collected without a warrant by the FBI in an incident unrelated to the NSA program. See Declan McCullagh, *Feds Push for Tracking Cell Phones*, CNET NEWS (Feb. 11, 2010, 4:00 AM), http://news.cnet.com/8301-13578_3-10451518-38.html

2011] The Fourth Amendment in the Age of Google 161

Despite this, the information an entity such as an email and information provider possesses on a single user conceivably can be enough to convict them or to create an arbitrary and embellished character profile of an individual. For example, incriminating web searches, emails, documents, photos, location data, and even evidence of acquaintanceship can be extracted from a user account.³⁶

B. Privacy and Fourth Amendment concerns in the age of Google

Citizens increasingly are trusting private companies with personal information in exchange for innovative, and sometimes necessary,³⁷ services. For decades banks have been entrusted with sensitive personal information about their clients in order to facilitate financial transactions.³⁸ Shortly after the attacks of September 11, 2001, lawsuits were launched against airlines for turning over private passenger information to government contractors.³⁹ In 2003, the FBI requested personal data from hotels, rental-car agencies and airlines in an effort to thwart then-looming Las Vegas terrorist threats.⁴⁰ In some instances,

[hereinafter *Feds Push for Tracking Cell Phones*] (demonstrating that while collected phone data does not fulfill the elements of the specific crime, it can be used in drawing an inference about the defendant's connection to the crime).

³⁶ See, e.g., Julia Lewis, *Petricks Prosecutors to Reopen Case with New Computer Evidence*, WRAL.COM (Nov. 28, 2005), <http://www.wral.com/news/local/story/122105/> (explaining how evidence gathered from Google searches was used in a trial against a man who allegedly killed his wife); Kim Zetter, *NSA-Intercepted E-Mails Helped Convict Would-Be Bombers*, WIRED.COM (Sept. 8, 2009, 6:26 PM), <http://www.wired.com/threatlevel/2009/09/nsa-email/> (explaining how evidence gathered by the NSA from email user accounts was passed to British prosecutors and presented at trial to convict three airplane bomb plotters). See also U.S. DEP'T OF HOMELAND SEC., BEST PRACTICES FOR SEIZING ELECTRONIC EVIDENCE (3d ed.), available at <http://www.forwardedge2.com/pdf/bestpractices.pdf> (characterizing the types of electronic evidence seized according to the crimes they are associated with).

³⁷ An email address has become almost as ubiquitous as a home address for employment, education, and billing purposes.

³⁸ See PETER REUTER & EDWIN M. TRUMAN, CHASING DIRTY MONEY: THE FIGHT AGAINST MONEY LAUNDERING 49–56 (2004) (examining the history of the anti-money laundering regime and the laws passed in the United States effectuated to prevent money laundering).

³⁹ Drew Shenkman, Comment, *Flying the Not-So-Private Skies: How Passengers' Personal Information Privacy Stopped at the Airplane Door, and What (If Anything) May Be Done To Get It Back*, 17 ALB. L.J. SCI. & TECH. 667, 668–70 (2007).

⁴⁰ Ellen Nakashima, *From Casinos to Counterterrorism*, WASH. POST, Oct. 22, 2007, <http://www.washingtonpost.com/wp-dyn/content/article/2007/10>

the data was voluntarily handed over.⁴¹ The Department of Defense even undertook a data-mining venture called the Total Information Awareness Project, which was later defunded by Congress.⁴² Now, the number of industries accumulating such information is more numerous, and the scope of inquiries is exponentially wider.⁴³

Although much attention has focused on controversies surrounding telephone company cooperation with the NSA, any of the most popular information service providers, such as Google, Microsoft, or Yahoo!,⁴⁴ could just as easily hand over user data from emails, calendars, voicemails, phone and instant message logs, web keyword searches, or photos. Government agencies already have used administrative subpoenas such as national security letters to compel disclosure of subscriber information.⁴⁵ Yet, consumers do not definitively waive Fourth Amendment rights merely by clicking “I agree” to an end-user license agreement. Nonetheless, private companies are not restrained as state actors when they voluntarily hand consumer data to the government. Instead, they are treated as a third party in whom a consumer is placing their trust.

Google perhaps epitomizes the data accumulation trend more

/21/AR2007102101522.html

⁴¹ *Id.*

⁴² John Markoff, *Pentagon Plans a Computer System That Would Peek at Personal Data of Americans*, N.Y. TIMES, Nov. 9, 2002, <http://www.nytimes.com/2002/11/09/politics/09COMP.html?scp=1&sq=Pentagon%20Plans%20a%20Computer%20System%20That%20Would%20Peek%20at%20Personal%20Data%20of%20Americans&st=cse>; Mark Williams, *The Total Information Awareness Project Lives On*, TECH. REV., (Apr. 26, 2006), <http://www.technologyreview.com/Infotech/16741/?a=f> (stating that Congress terminated funding of the Total Information Awareness Project but conditionally allows funding for projects involving component technology used for foreign intelligence or military use against non-U.S. citizens).

⁴³ For a thorough discussion of the Fourth Amendment issues surrounding government contractors and private-sector data-mining services, see Christopher Slobogin, *Government Data Mining and the Fourth Amendment*, 75 U. CHI. L. REV. 317, 319–21, 336–40 (2008).

⁴⁴ See Mark Brownlow, *Email and Webmail Statistics*, EMAIL MKTG. REPS. (Apr. 2008), <http://www.email-marketing-reports.com/metrics/email-statistics.htm>.

⁴⁵ See Joshua A. Altman, Note, *A Schrodinger's Onion Approach to the Problem of Secure Internet Communications*, 7 WASH. U. GLOB. STUD. L. REV. 103, 123–25, 128, 130 (2008). Moreover, the Patriot Act allowed mere administrative requests via national security letters to compel ISPs to turn over user data without user knowledge or judicial oversight. *Id.* at 126–28; 18 U.S.C. § 2703 (2010).

2011] **The Fourth Amendment in the Age of Google** 163

than any other private entity.⁴⁶ Google's profit model is based on offering free services to consumers in exchange for their consent to non-negotiable terms of service.⁴⁷ The services provided by Google encourage users to submit information that is organized and utilized to provide innovative and efficient means of online communication and digital media interaction.⁴⁸ However, Google's advertising system even tracks users' web browsing habits when they stray from Google's own website.⁴⁹ The information collected by Google allows the company to sell targeted advertising spots. Thus, the more information Google has about a user, the better the company can tailor the ads and increase their value.

Aside from tracking search and web browsing habits, Google also amasses data on emails, photos, healthcare records, phone calls, voicemails, and documents created on and sent through its servers.⁵⁰ Additionally, Google and similar companies boast the ability to pinpoint a user's exact location via their Internet Protocol address or through cell phone triangulation, allowing users to share this data with their friends.⁵¹ Thus, the

⁴⁶ Although Facebook might have more personal details about users and lax privacy concerns, users are opting to share much of this information with other users. See Sharon Gaudin, *Q&A: Facebook Users Aren't Outraged Over Privacy Issues*, NETWORK WORLD (May 7, 2010, 6:22 AM), <http://www.networkworld.com/news/2010/050710-qa-facebook-users-arent-outraged.html>. A Google account, on the other hand, is seemingly private unless users opt into sharing specific documents or photo albums. See *Frequently Asked Questions for the Google Analytics Data Sharing Options*, GOOGLE ANALYTICS, <http://www.google.com/support/analytics/bin/answer.py?hl=en&answer=87515> (last visited Nov. 29, 2010).

⁴⁷ See *Google Terms of Service*, GOOGLE (Apr. 16, 2007), <http://www.google.com/accounts/TOS>.

⁴⁸ See *Privacy Principles*, GOOGLE, http://www.google.com/corporate/privacy_principles.html (last visited Nov. 29, 2010) (stating that Google uses the information its users share to "build services and products that are valuable to them").

⁴⁹ Murad Ahmed, *Google Ad Service Raises Privacy Fears*, TIMES (London), Mar. 11, 2009, http://technology.timesonline.co.uk/tol/news/tech_and_web/article5887701.ece.

⁵⁰ See *About Google Voice*, GOOGLE VOICE, <http://www.google.com/support/voice/bin/answer.py?hl=en&answer=115061> (last visited Nov. 29, 2010); *About Google Health*, GOOGLE HEALTH, <http://www.google.com/intl/en-US/health/about/index.html> (last visited Nov. 29, 2010); *More Google Products*, GOOGLE, <http://www.google.com/intl/en/options/> (last visited Nov. 29, 2010).

⁵¹ See Stephen E. Henderson, *Learning From All Fifty States: How to Apply the Fourth Amendment and its State Analogs to Protect Third Party Information from Unreasonable Search*, 55 CATH. U. L. REV. 373, 381-85 (2006) (describing the advantages of refined location tracking). Yahoo also offers a location awareness service. *Yahoo Launches Latitude-like App for Facebook*,

accumulation of a citizen's email, documents, voicemails, phone logs, records, photos, and even location by Google rivals and perhaps exceeds the data gathering capabilities of traditional law enforcement methods. Google's database of consumer information is valuable to an outside government entity or advertiser. However, the aggregate of data collected on a person is even more invasive when analyzed to create a profile of a user's habits.⁵²

The synthesis of data from a user's web search history coupled with email, photos, documents, voicemails, phone logs, and location, creates a profile of an individual that serves as behavior modeling for advertisers.⁵³ This same data could just as easily be disclosed to law enforcement officials for criminal profiling. Social networking sites such as MySpace and Facebook likewise create additional privacy concerns. However, in these instances a user often controls who can view their information, although such a company potentially could voluntarily disclose such information to a law enforcement entity.⁵⁴ The United Kingdom is already considering plans to use data obtained by such sites to monitor users and prevent terrorism and crime.⁵⁵ Additionally, it is alleged that Google employees have met with members of the National Security Council to discuss potential collaborations.⁵⁶

TECHTREE.COM (Mar. 17, 2009, 2:54 PM), http://www.techtree.com/India/News/Yahoo_Launches_Latitude-like_App_for_Facebook/551-100105-580.html (Fire Eagle from Yahoo allows Facebook users to share their location with friends). Google recently confirmed that it was logging WLAN routers and MAC addresses. Kevin J. O'Brien, *New Questions over Google's Street View in Germany*, N.Y. TIMES, Apr. 29, 2010, <http://www.nytimes.com/2010/04/30/technology/30google.html>.

⁵² See Steve Lohr, *How Privacy Vanishes Online*, N.Y. TIMES, Mar. 16, 2010, <http://www.nytimes.com/2010/03/17/technology/17privacy.html> (discussing the "power of computers to identify people from social patterns").

⁵³ See Ira S. Rubinstein et al., *Data Mining and Internet Profiling: Emerging Regulatory and Technological Approaches*, 75 U. CHI. L. REV. 261, 261-63, 272 (2008) (explaining how data mining and profiling work).

⁵⁴ See Eric Kuhn, *Senators Urge Facebook to Change Privacy Settings*, CNN.COM (Apr. 28, 2010), <http://edition.cnn.com/2010/POLITICS/04/27/senators.facebook/index.html> (explaining that Facebook recently drew the ire of members of the U.S. Senate when it made previously private user data public).

⁵⁵ Murray Wardrop, *Facebook Could Be Monitored by the Government*, TELEGRAPH, Mar. 25, 2009, <http://www.telegraph.co.uk/technology/facebook/5046447/Facebook-could-be-monitored-by-the-government.html>.

⁵⁶ Byron Acohido, *Consumer Advocacy Group Calls for Hearing on Alleged Google Spying*, USA TODAY, July 20, 2010, <http://content.usatoday.com/communities/technologylive/post/2010/07/consumer-advocacy-group-calls-for-hearing-on-google-spying/1>.

2011] The Fourth Amendment in the Age of Google 165

Private data is amassed not only by many different companies but also is dispersed lawfully, unlawfully, and by accident.⁵⁷ Even traditional law enforcement means of retrieving online data by subpoenas is not limited merely to requests for relevant data from individual accounts. In 2005, the Department of Justice issued subpoenas to Google, America Online, Yahoo!, and Microsoft to compel the release of randomly selected user search records.⁵⁸ The DOJ's request was not intended to help solve a crime or prevent a terrorist attack.⁵⁹ Instead the data was requested for analytical purposes to support a new attempt to pass Internet child protection legislation.⁶⁰ While AOL and Yahoo! complied, Google remained defiant and refused to abide by the request.⁶¹

In *Gonzales v. Google*, the Department of Justice sued the Internet search giant for its failure to comply with the subpoena.⁶² Among other things, Google argued that even randomly selected search strings could be revealing if a user searched for their own name, social security number, or credit card number.⁶³ Additionally, Google argued that its business was predicated on protecting its users' privacy.⁶⁴ The U.S. District Court for the Northern District of California was quick to point to Google's own privacy policy, which did not protect users' search strings but merely their personal information.⁶⁵ Nonetheless, the court acknowledged that the fact that a quarter of all web searches are for pornography was evidence that there exists some expectation of privacy by at least some users.⁶⁶ In the end, Google was compelled only to generate a list of URLs, rather than actual user search queries.⁶⁷

Although marketplace and public relations forces likely

⁵⁷ See Karim Z. Oussayef, Note, *Selective Privacy: Facilitating Market-Based Solutions to Data Breaches by Standardizing Internet Privacy Policies*, 14 B.U. J. SCI. & TECH. L. 104, 112–14, 116, 118 (2008).

⁵⁸ *Latest Google Lawsuits*, LINKS & LAW.COM (Apr. 4, 2006), <http://www.linksandlaw.com/news-update38.htm>; Katie Hafner & Matt Richtel, *Google Resists U.S. Subpoena of Search Data*, N.Y. TIMES, Jan. 20, 2006, <http://www.nytimes.com/2006/01/20/technology/20google.html>.

⁵⁹ *See id.*

⁶⁰ *Id.*

⁶¹ *Id.*

⁶² *Gonzales v. Google, Inc.*, 234 F.R.D. 674, 678 (N.D. Cal. 2006).

⁶³ *Id.* at 687.

⁶⁴ *See id.* at 683.

⁶⁵ *Id.* at 683–84.

⁶⁶ *Id.* at 684.

⁶⁷ *Id.* at 688.

influenced Google's willingness to comply with a non-investigative government request, Google and other companies might not always feel so restrained. In 2006, America Online (AOL) released data on its customers' search queries for academic purposes. However, the data was matched with unique identifying numbers that could be used to pinpoint a user's identity.⁶⁸ One revelation from the data was that of a user whose searches "morphed over several weeks from 'you're pregnant he doesn't want the baby' to 'foods to eat when pregnant' to 'abortion clinics charlotte nc' to 'can christians be forgiven for abortion.'"⁶⁹ Thus, the potential for exposure of personal, non-national security related information is apparent.

In reference to the NSA warrantless surveillance program, Yahoo! refused to disclose whether or not it released user data to the government, citing only that it complied with its own privacy policy.⁷⁰ Moreover, it was recently revealed that Project Vigilant, a private group of hackers who cooperate with the federal government, receives traffic data from ISPs.⁷¹ The ISPs voluntarily hand over the data about their customers on the basis of End User License Agreements (EULA), which give them permission to do so, and Project Vigilant passes information onto the federal government.⁷² Therefore, any privacy interests that may exist are circumvented through a contract of adhesion. These examples demonstrate that the prospect of companies voluntarily providing seemingly-private information to the government is not merely a hypothetical but an increasingly-likely reality.

⁶⁸ Paul Boutin, *You Are What You Search*, SLATE MAG. (Aug. 11, 2006, 5:30 PM), <http://www.slate.com/id/2147590/>. See also Michael Barbaro & Tom Zeller Jr., *A Face Is Exposed for AOL Searcher No. 4417749*, N.Y. TIMES, Aug. 9, 2006, http://www.nytimes.com/2006/08/09/technology/09aol.html?_r=1 (The New York Times tracked down an AOL user based on her "anonymous" number and asked her about her searches).

⁶⁹ See Boutin, *supra* note 68.

⁷⁰ Declan McCullagh, *Yahoo on NSA surveillance: No comment*, CNET NEWS (Feb. 15, 2006, 1:55 PM), http://news.cnet.com/Yahoo-on-NSA-surveillance-No-comment/2100-1030_3-6040129.html.

⁷¹ Andy Greenberg, *Stealthy Government Contractor Monitors U.S. Internet Providers, Worked with Wikileaks Informant*, FORBES BLOGS (Aug. 1, 2010, 5:44 PM), <http://blogs.forbes.com/firewall/2010/08/01/stealthy-government-contractor-monitors-u-s-internet-providers-says-it-employed-wikileaks-informant/>.

⁷² *Id.*

IV. STATUTORY PROTECTIONS FOR ONLINE DATA

The Electronic Communications Privacy Act (ECPA) affords some privacy guarantees to users of electronic communications by establishing a regime of legal protections for users of any electronic communication service (ECS) or remote computing service (RCS).⁷³ The law, originally passed in 1986, is a statutory supplement to the Fourth Amendment's third party and private actor doctrines, placing restrictions only on services offered to the public.⁷⁴ The ECPA provided a potential cause of action for plaintiffs who sued phone companies that participated in the NSA's warrantless surveillance program until immunity was granted.⁷⁵

Comprised of three main parts, the codified statute incorporates the laws regarding the Wiretap Act, the Stored Communications Act (SCA), and the use of pen register information.⁷⁶ The U.S. Court of Appeals for the First Circuit interpreted interception of email stored during the communication process to fall under the wiretap provisions of the ECPA.⁷⁷ If this is accepted, then the government is required to obtain a warrant authorized by the Department of Justice and certified by a federal judge in order to intercept such communications.⁷⁸ However, if modern-day server-based email content is not analogized to fully-protected voice content then the lesser protections of the Stored Communications Act apply. The SCA merely requires a court order issued upon a reasonable belief that the material requested will be relevant to the investigation, thus falling short of a probable cause burden.⁷⁹

Although aspects of Google and other popular commercial services fall into the ECPA public communication category, other parts of the 1986-era definitions are ambiguous when applied to web-based services such as email.⁸⁰ An electronic communication service (ECS) is defined as "any service which provides to users thereof the ability to send or receive wire or electronic

⁷³ 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. 1208, 1208, 1214 (2004).

⁷⁴ *See id.* at 1212.

⁷⁵ *See* 18 U.S.C. § 2511 (2010).

⁷⁶ *See id.* §§ 2701–03; Kerr, *supra* note 73 at 1208 nn.1–2, 1231 n.151.

⁷⁷ *United States v. Councilman*, 418 F.3d 67, 79 (1st Cir. 2005).

⁷⁸ 18 U.S.C. §§ 2516–18 (2010).

⁷⁹ *See id.* § 2703(d).

⁸⁰ Kerr, *supra* note 73, at 1216–18.

communications.”⁸¹ Communications that are sent within the past 180 days fall under this definition. However, after 180 days then such communications are considered part of a remote computing service (RCS).⁸² The government cannot compel disclosure of user content data, such as unopened email,⁸³ from an ECS within this 180-day period without a warrant. However, the government can compel an RCS provider to release content information without use of a warrant, instead relying only on a subpoena and notice to the subscriber or an 18 U.S.C. § 2703(d) statutory order and prior notice.⁸⁴

The pre- and post-180 day distinctions stem from the concept that email originally was stored only temporarily on third party servers when in route from sender to receiver. This is no longer the case today with web-dependent cloud computing services such as Gmail, Yahoo! and Hotmail. Neither a public ECS nor RCS is permitted to voluntarily disclose content-laden data⁸⁵ to the government unless there is a § 2702(b) exception such as a good faith belief that “an emergency involving danger of death or serious physical injury” is imminent.⁸⁶ However, an ECS or RCS is permitted to divulge the contents of the electronic communication to another party with the permission of the subscriber of the service.⁸⁷ Moreover, the envelope information regarding who sent the email along with billing records are subject only to the aforementioned pen-register administrative subpoena requirements.⁸⁸

Today, many websites require user accounts and permanently store both content and non-content user information. Despite

⁸¹ 18 U.S.C. § 2510(15).

⁸² JAMES A. ADAMS, THE NAT’L INST. FOR TRIAL ADVOCACY, OVERVIEW OF CHAPTER 121. STORED WIRE AND ELECTRONIC COMMUNICATIONS AND TRANSACTIONAL RECORD ACCESS (2010).

⁸³ There is a dispute as to whether or not this covers opened mail as well. The U.S. Court of Appeals for the Ninth Circuit afforded opened emails with the same protections as unopened emails in electronic storage. *See Theofel v. Farey-Jones*, 341 F.3d 978, 985 (9th Cir. 2003). However, other courts disagree with this interpretation, and reason that opened emails can be divulged merely through the subpoena process. *See United States v. Weaver*, 636 F. Supp. 2d 769, 773 (C.D. Ill. 2009).

⁸⁴ Kerr, *supra* note 73, at 1223.

⁸⁵ Content data would include email. This is distinguished from non-content data such as a subscriber’s name and address, which is more akin to a pen register.

⁸⁶ 18 U.S.C. § 2702(b)(8) (2010).

⁸⁷ *See id.* § 2702(b)(3).

⁸⁸ *See supra* Part II; 18 U.S.C. § 2703(d).

2011] The Fourth Amendment in the Age of Google 169

this, the application of the Electronic Communications Privacy Act is not obvious. In *Re Jet Blue Airways Corp.*, the U.S. District Court for the Eastern District of New York held that the mere fact that Jet Blue provided a website and web service did not qualify the company as a provider under the definition of the ECPA.⁸⁹ Even the restrictions placed on relevant services by the ECPA are ambiguous. In *Freeman v. America Online*, the Connecticut Federal District Court interpreted the language in the ECPA broadly not only to restrict when the government can *require* information from ISPs, but also to prevent the government from *merely seeking* such information without adhering to the provisions of the statute.⁹⁰

The Electronic Communications Privacy Act fails to sufficiently protect the privacy rights of users of web-based services such as Gmail, Hotmail, Yahoo! Mail, etc.⁹¹ A Google account could conceivably be both an ECS and an RCS.⁹² However, much of its appeal is in its RCS functions because email, documents, photos, search histories, and more are all stored on a Google server, not a user's home computer. Thus, potentially personal and private documents or emails older than 180 days could be disclosed to law enforcement officers without any probable cause or warrant threshold.⁹³ Moreover, the Terms of Service agreements to which users assent might trigger the subscriber consent exception to the ECPA if the language is worded in such a way as to allow for voluntary disclosure. Due to the ECPA's seemingly ambiguous

⁸⁹ *In re JetBlue Airways Corp. Privacy Litig.*, 379 F. Supp. 2d 299, 307, 309-10 (E.D.N.Y. 2005).

⁹⁰ *Freedman v. Am. Online, Inc.*, 303 F. Supp. 2d 121, 127 (D. Conn. 2004).

⁹¹ For a thorough discussion of the ECPA's inadequacies see Achal Oza, *Amend the ECPA: Fourth Amendment Protection Erodes as E-mails Get Dusty*, 88 B.U. L. REV. 1043, 1068-73 (2008).

⁹² The U.S. Court of Appeals for the Ninth Circuit has categorized a service hosting opened email on its service as an ECS and some other courts have adopted this position. However, many academics criticize the position as inconsistent with the intent of the legislation. William Jeremy Robison, *Free at What Cost?: Cloud Computing Privacy Under the Stored Communications Act*, 98 GEO. L.J. 1195, 1211-12 (2010).

⁹³ Forced compliance with a subpoena by the service provider may occur even if the service provider believes its users have stronger legal protections. Microsoft, for example, interprets opened and unopened email to have the same protections. See Ryan Singel, *Microsoft Takes Down Whistleblower Site, Read the Secret Doc Here*, WIRED.COM (Feb. 24, 2010, 7:03 PM), <http://www.wired.com/threatlevel/2010/02/microsoft-cryptome/>. However, Microsoft has still been forced to violate its own privacy policies and comply with a subpoena. See also *Unites States v. Weaver*, 636 F. Supp. 2d 769, 773 (C.D. Ill. 2009).

application to the modern World Wide Web, Congress has held hearings on updating the law – a cause that has received broad support from the service provider community, including Microsoft, Google, and Yahoo!.⁹⁴ Regardless of the statutory regime, constitutional issues persist.

V. “DIGITAL PAPERS” AND “EFFECTS”?

A. *Expectation of Privacy*

Justice Louis Brandeis, in a dissenting opinion in *Olmstead v. United States*, predicted that “[w]ays may some day be developed by which the Government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home.”⁹⁵ This once farfetched notion is now a reality as Americans’ papers go digital. The dawn of cloud computing has arrived, and the attractiveness of data-portability means that individuals are migrating their personal documents from in-home hard drives to the machines of remote third parties.⁹⁶ With this trend, people are expanding their privacy expectations from the physical confines of their home to that of password-protected accounts for everything from online banking to Internet-based word processing.⁹⁷ Users even divulge personal information with

⁹⁴ Nancy Scola, *A 21st-Century Fourth Amendment*, THE AMERICAN PROSPECT, TAPPED BLOG (Mar. 31, 2010, 2:04 PM), http://www.prospect.org/cs/n/blogs/tapped_archive?month=03&year=2010&base_name=a_21st_century_4th_amendment.

⁹⁵ *Olmstead v. United States*, 277 U.S. 438, 474 (1927) (Brandeis, J., dissenting) (predicting that technological innovations would soon lead the Court to the opposite conclusion). See also *Katz v. United States*, 369 U.S. 347, 358–59 (1967) (holding electronic surveillance of a telephone booth requires prior authorization and a showing of probable cause).

⁹⁶ Google is entering a market already populated by other vendors. See Kevin J. Delaney & Vauhini Vara, *Google Plans Service to Store Users’ Data*, WALL ST. J., Nov. 27, 2007, <http://online.wsj.com/article/SB119612660573504716.html>.

⁹⁷ As of 2008, 69% of Americans were using cloud computing services, with more than half using web-based mail and a third storing their photos or files online. Fawn Johnson, *Most People Who Store Data on Web Want It Private - Study*, DOWJONES VENTUREWIRE (Sept. 15, 2008), http://fis.dowjones.com/products/vw_sample.html. According to a 2010 Zogby International poll, 88% of American adults believe they should be afforded the same privacy protections online as they receive offline. See ZOGBY INT’L, RESULTS FROM JUNE 4-7 NATIONWIDE POLL 1 (June 7, 2010), available at <http://www.precursorblog.com/files/pdf/topline-report-key-findings.pdf>. The notion of a password protected and encrypted online account is akin to a locked container and therefore

2011] The Fourth Amendment in the Age of Google 171

an expectation of privacy when conducting search engine queries.⁹⁸ However, current case law leaves more questions than answers about the extent of Fourth Amendment protections.

A central issue in applying the Fourth Amendment to technology is determining what is content versus non-content and what a person reasonably expects to remain private. The Court held in *Smith v. Maryland* that a mere list of the phone numbers dialed by a caller is not protected content data.⁹⁹ By analogy, email to and from headers as well as IP addresses were interpreted by the U.S. Court of Appeals for the Ninth Circuit to be the same as unprotected pen register data.¹⁰⁰ However, the U.S. Supreme Court hinted in *City of Ontario, Cal. v. Quon* that the pervasiveness of cell phones might strengthen the case for a reasonable expectation of privacy in the content of text messages.¹⁰¹ For content, the Court applies the Fourth Amendment test from Justice John Harlan's concurring opinion in *Katz v. United States*,¹⁰² which was adopted by the majority in *Smith*, providing a two-pronged defense against Fourth Amendment intrusion.¹⁰³ First, an individual must exhibit a subjective expectation of privacy in their relevant activity or communication.¹⁰⁴ Second, the expectation must be one that society is willing to accept as legitimate.¹⁰⁵

At present, the Supreme Court has been reluctant to recognize an express privacy interest in electronic communication, going so far as to assume the existence of privacy interests in cell phone

deserves Fourth Amendment protections. Sean J. Edgett, *Double-Clicking on Fourth Amendment Protection: Encryption Creates a Reasonable Expectation of Privacy*, 30 PEPP. L. REV. 339, 364–65 (2003). A federal district court initially found an expectation of privacy in a user's Yahoo! email account despite arguments from the U.S. government that the petitioner had no reasonable expectation of privacy. However, the U.S. Court of Appeals for the Sixth Circuit vacated the decision on ripeness grounds. *Warshak v. United States*, 532 F.3d 521, 523 (6th Cir. 2008).

⁹⁸ Matthew Werner, *Google and Ye Shall be Found: Privacy, Search Queries, and the Recognition of a Qualified Privilege*, 34 RUTGERS COMPUTER & TECH. L.J. 273, 300–01 (2007). Additionally, as previously mentioned in the article, even Google defended the privacy of search strings when the DOJ requested them. See *supra* Part I.b.

⁹⁹ See *Smith v. Maryland*, 442 U.S. 735, 744 (1979).

¹⁰⁰ *United States v. Forrester*, 512 F.3d 500, 504 (9th Cir. 2007).

¹⁰¹ 130 S.Ct. 2619, 2630 (2010).

¹⁰² *Katz v. United States*, 389 U.S. 347, 361–63 (1967) (Harlan, J., concurring).

¹⁰³ *Smith*, 442 U.S. at 740–41.

¹⁰⁴ *Id.* at 740 (citing *Katz*, 389 U.S. at 361 (Harlan, J., concurring)).

¹⁰⁵ *Id.*

text messages merely *arguendo* to decide a case on much narrower grounds.¹⁰⁶ While certain information in the hands of third parties, such as traditional business records, is not afforded Fourth Amendment protection equivalent to “papers” or “effects,”¹⁰⁷ there is ambiguity over the constitutional protection afforded to private email or online documents.¹⁰⁸

A federal district court in Rhode Island found that a Yahoo! email account user had a reasonable expectation of privacy in their password-protected account despite the fact that the user accessed it from a public library.¹⁰⁹ However, if higher courts adopt a narrower standard of privacy, then a user’s location might be a decisive factor. A web-based email user does not need to access their documents in public. Instead, consumers of Gmail, Google Docs, and other services are just as likely to view and modify their personal files from the confines of their own home. Traditionally more Fourth Amendment protection has been afforded to the home. Police cannot use a beeper to track the movements of a person within their own home without a warrant.¹¹⁰ Nor can police use thermal imaging devices to conduct a remote warrantless search of a home.¹¹¹ By analogy, a user should, at the bare minimum, have a reasonable expectation of privacy in their home even when accessing their digital documents and effects, whether or not the data is local.¹¹²

On the contrary, location data is used by Google’s email service, Gmail, when scanning information and text contained in

¹⁰⁶ See *City of Ontario, Cal.*, 130 S. Ct. at 2630.

¹⁰⁷ See U.S. CONST. amend. IV. See also Seth Rosenbloom, *Crying Wolf in the Digital Age: Voluntary Disclosure Under the Stored Communications Act*, 39 COLUM. HUM. RTS. L. REV. 529, 534–35 (2008).

¹⁰⁸ See generally, *United States v. Bach*, 310 F.3d 1063, 1066 (8th Cir. 2002) (explaining when email files are protected under the Fourth Amendment); Kerr, *supra* note 72, 1210–12 (outlining three reasons why the Fourth Amendment does not afford protections for online documents); Stephen E. Henderson, *Nothing New Under the Sun? A Technologically Rational Doctrine of Fourth Amendment Search*, 56 MERCER L. REV. 507, 522 (2005) (detailing that courts have yet to clarify if the “sender of email[s] retain[] a reasonable expectation of privacy . . .”).

¹⁰⁹ See *Wilson v. Moreau*, 440 F. Supp. 2d 81, 108 (D.R.I. 2006).

¹¹⁰ See *United States v. Karo*, 468 U.S. 705, 717–18 (1984).

¹¹¹ *Kyllo v. United States*, 533 U.S. 27, 37, 40 (2001).

¹¹² Alternatively, a person does not always enjoy a reasonable expectation of privacy in their location data. At present, the Obama administration argues that individuals enjoy no expectation of privacy in the location of their cell phones. See *Feds Push for Tracking Cell Phones*, *supra* note 35.

2011] The Fourth Amendment in the Age of Google 173

email and documents to generate relevant advertisements.¹¹³ Therefore, such a knowing relinquishment of information might affect a *Katz*-analysis of a person's reasonable expectation of privacy and perhaps be analogous to items in the plain view of the public. Or, alternatively, the Internet Protocol location data indicating that a person is in their home might afford them greater Fourth Amendment protection when they are home. However, these concepts ignore the fact that although individuals might voluntarily allow their data to be scanned by an automatic system that generates tailored advertisements for their eyes only, it is not a foregone conclusion that they are therefore consenting to unfettered law enforcement or personified third party access to their data. Moreover, a person's privacy in their documents and effects should hinge more on their property and privacy interests in the documents and effects, rather than their technical location. Thus, password-protected, encrypted digital storage containers should be a Fourth Amendment-protected place to store the "most intimate occurrences of the home."¹¹⁴

B. Third-party doctrine

This Court has held repeatedly that the 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.¹¹⁵

The Supreme Court has held that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."¹¹⁶ Such a blanket concept is troublesome enough when dealing with issues of "shared privacy" between individuals.¹¹⁷ However, the doctrine appears

¹¹³ Laura Rohde, *GMail Still Dogged by Privacy Issues*, COMPUTERWEEKLY.COM (Apr. 16, 2004, 10:33AM), <http://www.computerweekly.com/Articles/2004/04/16/201808/Gmail+still+dogged+by+privacy+issues.htm>.

¹¹⁴ *Olmstead v. United States*, 277 U.S. 438, 474 (1928) (Brandeis, J., dissenting).

¹¹⁵ *United States v. Miller*, 425 U.S. 435, 443 (1976).

¹¹⁶ *Smith v. Maryland*, 442 U.S. 735, 743–44 (1979). This sentiment is echoed in *S.E.C. v. Jerry T. O'Brien, Inc.* 467 U.S. 735, 743 (1984).

¹¹⁷ Mary I. Coombs, *Shared Privacy and the Fourth Amendment, or the*

increasingly archaic and problematic when the third party is a seemingly anonymous and automated online media service provider.¹¹⁸ The doctrine was articulated before digital documents and effects were stored in the cloud and should be distinguished from the relationship between a communication server provider and its users.

One argument promoted to limit this doctrine advances the notion that the Fourth Amendment third party test should relinquish protection only for information volunteered for a third party's use.¹¹⁹ However, Google scans virtually all text from user emails, documents, and searches to determine which advertisements to display.¹²⁰ Therefore, such a doctrine conceivably would fail to afford any Fourth Amendment protections to a user entrusting their data to a third party. Moreover, a user usually does not have standing to sue the government for taking information from a third party. The U.S. Court of Appeals for the Eleventh Circuit recently opined that "voluntary delivery of emails to third parties constituted a voluntary relinquishment of the right to privacy in that information" when dismissing a lawsuit against the government for subpoenaing the content of the plaintiff's emails from an ISP.¹²¹

The fact that the government was able to obtain the emails from the service provider, rather than the email recipient, without triggering the Fourth Amendment exemplifies the current problem. The Internet is run primarily by private entities beginning with the cable, telephone wire, or wireless network running into a user's home all the way to the webpage on a remote server accessed by their computer. Therefore, users interact with a myriad of digital third parties in every online activity from sending an email to navigating the Web. As such,

Rights of Relationships, 75 CALIF. L. REV. 1593, 1616–19 (1987).

¹¹⁸ Cracks have begun to emerge in the doctrine through some state constitutional protections, but the doctrine remains largely unchanged. See Stephen E. Henderson, *Learning from All Fifty States: How to Apply the Fourth Amendment and its State Analogs to Protect Third Party Information from Unreasonable Search*, 55 CATH. U. L. REV. 373, 412–13 (2006).

¹¹⁹ *Id.* at 378.

¹²⁰ Ira S. Rubinstein, Ronald D. Lee & Paul M. Schwartz, *Data Mining and Internet Profiling: Emerging Regulatory and Technological Approaches*, 75 U. CHI. L. REV. 261, 271–73 (2008); *More on Gmail and Privacy*, GOOGLE, http://mail.google.com/mail/help/about_privacy.html#scanning_email (last visited Nov. 29, 2010).

¹²¹ *Rehberg v. Paulk*, 598 F.3d 1268, 1282 (11th Cir. 2010).

2011] The Fourth Amendment in the Age of Google 175

users' expectations of privacy appear inconsistent with traditional notions of third-party "false friends" when applied to online communications.

A strong argument in favor of preserving the third-party doctrine is the necessity of maintaining the public parts of crimes and allowing evidence to come to light for investigation and prosecution.¹²² Even absent Fourth Amendment protection, other legal protections from "[c]ommon law privileges, entrapment law, the *Massiah* doctrine, First Amendment doctrine, and statutory privacy protections" offer some defenses for those targeted based on their Gmail accounts.¹²³ However, sidestepping the Fourth Amendment ignores the technological evolution of papers and effects in the digital era. Moreover, it fails to acknowledge that individuals might be willing to share their documents and effects with online service providers but not offer them for warrantless review by law enforcement entities. Therefore, the third-party doctrine should not be oversimplified.

A service provider's voluntary disclosure of users' emails and documents to the government might find support in the false friend theory. However, in *United States v. James*, the U.S. Court of Appeals for the Eighth Circuit rejected the government's claim that the defendant abandoned his privacy interests in a CD when he handed it to a third party with instructions to destroy it.¹²⁴ Moreover, the false friend notion is inconsistent with the distinctions drawn in *Smith v. Maryland* between subscriber data and a phone conversation itself.¹²⁵ An argument advanced in support of the third-party doctrine contends users divulging information to a third party "implies consent" under the Fourth Amendment.¹²⁶ However, this argument removes the reasonable expectation of privacy framework in exchange for a presumptive

¹²² See Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 564–65 (2009).

¹²³ *Id.* at 565.

¹²⁴ See 353 F.3d 606, 616 (8th Cir. 2003).

¹²⁵ The Fourth Amendment protects private conversations where the party has not consented to surveillance or monitoring, but not where the party has given consent to such activity, signifying the existence of a reasonable expectation of privacy. See *United States v. White*, 401 U.S. 745, 747, 749, 752–54 (1971). *C.f.*, *Smith v. Maryland* 442 U.S. 735, 742–44 (1979) (stating that Pen registers only record numbers, and not the content of the phone conversations. Since the Fourth Amendment applies only to privacy, recording phone numbers falls outside the gambit of a person's reasonable expectation of privacy).

¹²⁶ Kerr, *supra* note 122 at 565.

conclusion of search acquiescence. This argument is especially weak when the party is not a person but instead an automated digital document repository.

Contrary to traditional third party information exchanges, Google's "secure"¹²⁷ services might lead a user reasonably to believe that their contents are in a virtual closed container, justifying a reasonable expectation of privacy.¹²⁸ This analogy allows users reasonably to assume that their data is safe from unwarranted governmental intrusion even if Google's automated algorithms can access it for advertising purposes.¹²⁹ One could argue that users might reasonably risk betrayal by a service provider playing the role of a false friend. Moreover, users could reasonably expect that Google might read their email and disclose it to the government. However, the fact that a user protects their Google account, which contains email, documents, photos, location information, and more, with encryption and a password lends credence to both a subjective and perhaps objective expectation of privacy from both personal access by Google employees and unwarranted law enforcement access. Therefore, some authors have applied the analogy of a traditional closed container to encrypted, password-protected email.¹³⁰

The contents of a user's encrypted, password-protected account is beyond public view and is perhaps an extension of a filing cabinet in a private single-user home office or at least a locked container.¹³¹ Unlike a home dwelling, which a person may share

¹²⁷ Google advertises Gmail as a "secure" email service. *Gmail: Google's Approach to email*, GMAIL, <http://mail.google.com/mail/help/intl/en/about.html#faq> (last visited Nov. 29, 2010).

¹²⁸ A user might conceivably assume that "deleted" mail is inaccessible too. Such mail, however, can remain on both online third party servers as well as offline backups. See *Google Privacy Policy*, GOOGLE, <http://mail.google.com/mail/help/intl/en/privacy.html> (last visited Nov. 29, 2010); see generally, *Email, SURVEILLANCE SELF DEFENSE*, <https://ssd.eff.org/tech/email> (last visited Nov. 29, 2010) (discussing that e-mails can be stored in third party computers through channels such as the service provider, employers, ISP, webmail provider, or can be stored by those you communicate with).

¹²⁹ Google advertises that no human is involved in this email-scanning process. Thus, a user might not have a reasonable expectation of privacy from a computer that it might from a human. See *Ads in Gmail and Your Personal Data*, GMAIL HELP, <http://mail.google.com/support/bin/answer.py?hl=en&answer=6603> (last visited Nov. 29, 2010); see also Paul Hartsock, *HP's Wallet-Busting Win*, E-COM. TIMES, (Sept. 3, 2010, 9:58 AM), <http://www.ecommercetimes.com/story/70758.html?wlc=1285606130>.

¹³⁰ See e.g., Henderson, *supra* note 108 at 533-35.

¹³¹ Courts traditionally have found a reasonable expectation of privacy in locked containers and even unlocked containers. The password-protected aspect

2011] The Fourth Amendment in the Age of Google 177

with others, a user is likely the only individual with access to their account password.¹³² Thus, by analogy, emails and digital documents within the account should warrant the same Fourth Amendment protection as those in the locked storage container or locker. However, a rigid and technologically agnostic reading of the Fourth Amendment fails to extend the same protections when a user voluntarily chooses to put their documents online, in the hands of a third party cloud computing service. This is similar to some courts' view that the Fourth Amendment does not offer protection to users of certain types of technology, for example cell phones that broadcast personal information such as location data.¹³³ Yet, such an approach ignores users' expectations of privacy in the devices, which store their personal data. A person's digital papers and effects may be accessible from virtually anywhere.

If a U.S. person keeps their documents in the cloud on a remote server abroad, then the privacy reality might change. A U.S. company holding a U.S. person's papers and effects on a U.S. server abroad still would be governed by the statutory restrictions of the ECPA.¹³⁴ However, in the areas where the

of user accounts in the cloud-computing domain lends credence to a reasonable expectation of privacy with digital papers and effects. See David A. Couillard, *Defogging the Cloud: Applying Fourth Amendment Principles to Evolving Privacy Expectations in Cloud Computing*, 93 MINN. L. REV. 2205, 2209–11, 2218–19, 2224–27 (2009). Yet, the same author has analogized password-protected accounts to landlord tenant relationships because the landlord might have a limited right of entry but not unfettered access. *Id.* at 2236–38. This analogy is good as long as it is not dealing with a shared-dwelling. In that case, the locked container analogy would be more appropriate.

¹³² If the account was shared then this might be more akin to a shared residence in which any of the parties living at a place could grant consent. See *United States v. Matlock*, 415 U.S. 164, 169–70, 177 (1974) (holding a search that was conducted after another resident consented to search of the shared dwelling reasonable).

¹³³ Henderson, *supra* note 108 at 384–90.

¹³⁴ Google, among other companies, hosts their servers in various parts of the world. See, e.g., Rich Miller, *Google Data Center FAQ*, DATA CENTER KNOWLEDGE (Mar. 27, 2008), <http://www.datacenterknowledge.com/arc-hives/2008/03/27/google-data-center-faq/> (listing countries where Google has data centers that host servers, outside the U.S., such as in Germany, London, Netherlands, and Italy, to name a few); Charlie Savage, *U.S. Tries to Make it Easier to Wiretap the Internet*, N.Y. TIMES, Sept. 27, 2010, <http://www.nytimes.com/2010/09/27/us/27-wiretap.html?pagewanted=all> (listing Research Motion as a company that operates servers abroad); David Schellhase, Exec. Vice President & Gen. Counsel, Salesforce.com, Testimony before the U.S. House of Representatives: ECPA Reform and the Revolution in Cloud Computing 11 (Sep. 23, 2010), *available at*

ECPA is ambiguous, or in cases where a U.S. person is hosting their documents and effects with a company that does not operate from the U.S., then only constitutional protections triggered by a relevant search would apply.¹³⁵ If the country hosting the servers seizes the data for any reason, or if the company voluntarily discloses the data to another party, then the new party possessing the data conceivably could pass it on to U.S. law enforcement as a fourth party without ever triggering the Fourth Amendment or the ECPA.¹³⁶ From a tort and contractual standpoint, users might even explicitly acquiesce to or at least be on notice of such a possibility through their Terms of Service agreement.

VI. TERMS OF SERVICE: AN IMPLIED CONSENT?

The digital age has made consumer assent to contracts of adhesion-like terms, as found in the ubiquitous “Terms of Service” clauses (TOS).¹³⁷ Often, language in a TOS agreement merely disclaims liability for any damage to a user’s computer or data and forbids unauthorized use or redistribution of intellectual property. However, Terms of Service are not relegated to limits on consumer behavior. Such terms also dictate the terms by which the entity will retain, control, and own a user’s information. Thus, a user of free services is (often unbeknownst to them) effectively exchanging valuable personal information for the use of online services.¹³⁸

The fact that the terms of a website agreement are not negotiated does not diminish the enforceability of such Terms of

<http://judiciary.house.gov/hearings/pdf/Schellhase100923.pdf>.

¹³⁵ The Fourth Amendment reasonableness requirement, but not the warrant requirement, applies to searches of U.S. persons conducted overseas “when the participation of United States agents in the investigation is so substantial that the action is a joint venture between the United States and foreign officials.” *United States v. Stokes*, 710 F. Supp. 2d 689, 695–699 (N.D. Ill. 2009).

¹³⁶ According to the U.S. Court of Appeals for the Second Circuit, the “Fourth Amendment’s requirement of reasonableness and not the Warrant Clause governs extraterritorial searches of U.S. citizens.” This concept could therefore regulate a direct search or seizure of a server abroad by U.S. authorities. *In re Terrorist Bombings of U.S. Embassies in E. Afr.*, 552 F.3d 157, 159 (2d Cir. 2008).

¹³⁷ Cory S. Winter, *The Rap on Clickwrap: How Procedural Unconscionability is Threatening the E-Commerce Marketplace*, 18 WIDENER L.J. 249, 271–73 (2008).

¹³⁸ Nikki Tait & Tim Bradshaw, *EU to Probe Web User Profiling by Advertisers*, FIN. TIMES, Mar. 29, 2009, <http://www.ft.com/cms/s/0/ef387d70-1ca2-11de-977c-00144feabdc0.html>.

2011] The Fourth Amendment in the Age of Google 179

Service.¹³⁹ However, despite the popularity of broad TOS agreements for efficiency in the digital age, the non-dickered terms are not limitless and can be found unconscionable, particularly when there are no market alternatives to a service.¹⁴⁰ Yet, this is difficult to demonstrate in the search engine, email, and digital media services market, where there are many companies even though only a few giants dominate. Under the weak statutory protections of the Electronic Communications Privacy Act, the possibility of compelled subscriber permission provides law enforcement officers with a much easier avenue for retrieving digital rather than traditional evidence. The Fourth Amendment requirement of probable cause is a much higher threshold than the amorphous standards of using a subpoena, which does not always require court approval.¹⁴¹

A Title III order is required to obtain the contents of email in real time, which must be approved by the DOJ, granted by a federal judge, and renewed every 30 days.¹⁴² For stored, unopened email a traditional search warrant is required.¹⁴³ However, only a subpoena with notice is necessary for the government to compel the disclosure of opened emails or stored files. An *ex parte* pen register order is necessary for the government to obtain real time subscriber data,¹⁴⁴ but a mere subpoena is sufficient for past non-content subscriber information.¹⁴⁵ While these requirements appear to provide sufficient safeguards for users, protections for non-real time data are trumped by consent, and users may unwittingly consent to such disclosure.

Google requires that its users adhere to its Terms of Service or not use its products and services.¹⁴⁶ Google defines content as “as data files, written text, computer software, music, audio files or other sounds, photographs, videos or other images” which users

¹³⁹ See Ty Tasker & Daryn Pakcyk, *Cyber-Surfing on the High Seas of Legalese: Law and Technology of Internet Agreements*, 18 ALB. L.J. SCI. & TECH. 79, 90-91, 116-17 (2008).

¹⁴⁰ *Bragg v. Linden Research, Inc.*, 487 F. Supp. 2d 593, 606 (E.D. Pa. 2007).

¹⁴¹ William J. Stuntz, Commentary, *O.J. Simpson, Bill Clinton, and the Transsubstantive Fourth Amendment*, 114 HARV. L. REV. 842, 864 (2001).

¹⁴² 18 U.S.C. § 2518 (2010).

¹⁴³ See *id.* § 2703(a).

¹⁴⁴ *Id.* § 3123.

¹⁴⁵ *Id.* § 2703(d).

¹⁴⁶ *Google Terms of Service*, GOOGLE, <http://www.google.com/accounts/TOS> (last visited Nov. 29, 2010).

may access or use.¹⁴⁷ The company then claims “a perpetual, irrevocable, worldwide, royalty-free, and non-exclusive license to reproduce, adapt, modify, translate, publish, publicly perform, publicly display and distribute any Content which you submit, post or display on or through, the Services.”¹⁴⁸ However, the TOS agreement notes that certain services have different terms.

For example, users of Google’s Gmail service accept terms which dictate that Google might retain messages, even from deleted accounts, in its offline backup servers.¹⁴⁹ Moreover, Google states that it will not release personal information nor content except in “limited circumstances” described in its privacy policy and when Google believes it is “required [to do so] by law.”¹⁵⁰ Google’s exceptions include when they:

have a good faith belief that access, use, preservation or disclosure of such information is reasonably necessary to (a) satisfy any applicable law, regulation, legal process or enforceable governmental request, (b) enforce applicable Terms of Service, including investigation of potential violations thereof, (c) detect, prevent, or otherwise address fraud, security or technical issues, or (d) protect against harm to the rights, property or safety of Google, its users or the public as required or permitted by law.¹⁵¹

Google’s Gmail terms of service might appear reasonable for a free service even though the company’s umbrella privacy policy sounds frighteningly vague and seems to embolden Google with the power to do anything with a user’s data. Moreover, the company reserves the right to change the terms. Also, the fact that Google’s Terms of Service allow for disclosure of private information to advertisers emboldens the notion that a Fourth Amendment right against unlawful searches and seizures might belong to Google, but not to a Google user.¹⁵² Nevertheless,

¹⁴⁷ *Id.*

¹⁴⁸ *Id.*

¹⁴⁹ *Google Privacy Policy*, *supra* note 128.

¹⁵⁰ *Id.*

¹⁵¹ *Id.*

¹⁵² A recent example of Google’s malleable view on privacy was demonstrated with the launch of its new “Buzz” service, which automatically linked frequently emailed Gmail contacts to each other’s Twitter-like comment feeds and public photo albums. After much user uproar, the company was forced to convert these automatic connections to automatic suggestions. Jonathan Fildes, *Google Admits Buzz Social Network Testing Flaws*, BBC NEWS, Feb. 16, 2010, <http://news.bbc.co.uk/2/hi/technology/8517613.stm>; Hibah Yousuf, *Google Alters Buzz After Privacy Complaints*, CNNMONEY.COM (Feb. 15, 2010), http://money.cnn.com/2010/02/15/technology/Google_Buzz_privacy/index.htm?cnn=yes.

2011] The Fourth Amendment in the Age of Google 181

Google and other online service providers act as modern day document repositories for many people, harboring their papers and effects.¹⁵³ Despite this, it appears possible for a court to enforce a TOS agreement by which a user inadvertently contracts away their right to privacy.

The U.S. Court of Appeals for the Eleventh Circuit cited Federal Express' terms of service agreement as a main reason why a customer did not have a reasonable expectation of privacy in the contents of a package which FedEx allowed law enforcement authorities to search without a warrant. Another federal district court characterized promises regarding privacy rights in AOL's Terms of Service as merely "aspirational" because they did not "confer any rights or remedies" upon its users.¹⁵⁴ Thus, if a service provider is not bound by its own terms nor by the Fourth Amendment and users have no statutory protection then the government effectively can moot Fourth Amendment privacy protections through service provider cooperation.¹⁵⁵ However, if consent is defined by Fourth Amendment standards of expectations of privacy then users could remain protected regardless of the Terms of Service.

The number of cases in which courts have applied the Fourth Amendment to email remains limited. However, courts have applied the Fourth Amendment to a narrow set of circumstances. One prominent example is that of *United States v. Monroe*, in which the United States Court of Appeals for the Armed Forces held that a Fourth Amendment search did not occur when the government network administrator accessed a user's email, despite the government's role as the service provider for users of government computers.¹⁵⁶ This is due in part to the large disclaimer appearing on the screen when a user logs into a government computer.¹⁵⁷ However, the same court found that a

¹⁵³ As Google CEO Eric Schmidt notes, "[t]his is not a Google decision, this is a societal decision." Shane Richmond, *Google's Eric Schmidt: You Can Trust Us With Your Data*, TELEGRAPH, Jul. 1, 2010, <http://www.telegraph.co.uk/technology/google/7864223/Googles-Eric-Schmidt-You-can-trust-us-with-your-data.html>.

¹⁵⁴ *Freedman v. Am. Online, Inc.*, 325 F. Supp. 2d 638, 640 (E.D. Va. 2004).

¹⁵⁵ A possible safeguard against this scenarios lies within the state actor doctrine discussed later in this paper. A user might be able to restrain Google's actions on a constitutional basis if they can prove that the government actively encouraged Google to violate the user's Fourth Amendment or other constitutional rights.

¹⁵⁶ *United States v. Monroe*, 52 M.J. 326 (C.A.A.F. 2000).

¹⁵⁷ *Id.* at 327.

user did have an objectively reasonable subjective expectation of privacy in a similar case, *United States v. Long*.¹⁵⁸

In *Long*, the court's decision hinged on the fact that the network's Department of Defense computer disclaimer did nothing to erode a user's expectation of privacy in their email against law enforcement searches.¹⁵⁹ Instead, it merely implied that the computer usage reasonably was subjected to work-related non-criminal investigation monitoring.¹⁶⁰ Thus, it is possible, at least with a prominent enough notice and when the government is the service provider, for a user to agree to waive their Fourth Amendment protections in cyberspace. However, this is not automatically assumed, particularly when a notice fails to extinguish an objectively reasonable subjective expectation of privacy.

"Clickwrap" agreements are problematic in that they are often too ambiguous, too confusing, too obscure, or even too long for consumers to understand.¹⁶¹ Privacy policies by their very nature sometimes make consumers believe private protections are being bestowed upon them.¹⁶² The way in which Google products are marketed as a secure platform and the promotion of Google Docs as an alternative to desktop document processing exemplifies the likely expectations of consumers that their privacy is not being compromised.¹⁶³ Therefore, even though every user of these products and similar products must click through a TOS agreement, they might be expressing more of a willingness to use the product responsibly rather than an affirmative relinquishment of privacy. Even if a privacy policy puts a user on notice that their information might be analyzed, it is unlikely that users are on notice to the fact or accept the fact that their private information will receive less protection with

¹⁵⁸ *United States v. Long*, 64 M.J. 57, 59 (C.A.A.F. 2006).

¹⁵⁹ *Id.* at 63.

¹⁶⁰ *Id.* at 65.

¹⁶¹ Susan E. Gindin, *Nobody Reads Your Privacy Policy or Online Contract? Lessons Learned and Questions Raised by the FTC's Action Against Sears*, 8 NW. J. TECH. & INTELL. PROP. 1, 20, 48 (2009).

¹⁶² JOSHUA GOMEZ, TRAVIS PINNICK, & ASHKAN SOLTANI, UNIV. OF CAL. BERKELEY, SCH. OF INFO., KNOWPRIVACY 11 (2009), available at http://knowprivacy.org/report/KnowPrivacy_Final_Report.pdf.

¹⁶³ *Software-as-a-Service has Built-in Security Advantages*, GOOGLE APPS, http://www.google.com/apps/intl/en/business/infrastructure_security.html (last visited Nov. 29, 2010) (promoting the security of Google Apps, which includes products such as Google Docs, Google Calendar, and Gmail which are offered to the public for free).

2011] The Fourth Amendment in the Age of Google 183

regard to law enforcement. Moreover, it is sometimes difficult to ascertain with whom a user has an agreement and to whom a user gives up an expectation of privacy.¹⁶⁴

VII. “DON’T BE EVIL” TO “CAN’T BE EVIL”¹⁶⁵***A. The need to restrain third party service providers***

The porous statutory protections afforded to online data are inadequate for protecting citizens’ 21st century papers and effects. Similarly, current Fourth Amendment jurisprudence does not reflect the reasonable expectation of privacy maintained by those who trust their modern day papers and effects with third parties for commonplace electronic-age conveniences. Third parties increasingly have assumed capabilities previously held as a near monopoly by the state to conduct investigations and maintain private information about citizens.¹⁶⁶ However, electronic contracts of adhesion are limiting the private rights of an individual to protect their privacy in services so vital to daily life.

Current procedural safeguards are insufficient to prevent the government or even the third party service provider from trampling user privacy. Under normal circumstances, when records are subpoenaed, targeted parties may respond to a record request before such information is disclosed. Similarly, the Fourth Amendment generally requires that the government obtain a search warrant predicated on probable cause when compelling a private party to effectuate a search on its behalf. Thus, new challenges exist with regard to the NSA data

¹⁶⁴ Yale University recently contracted with Google to replace the school’s email client with a custom version of Gmail. This creates a potentially more complicated third-party scenario depending on by whose terms of service the students must abide and how the email service is managed and data is stored. See David Tidmarsh, *Google to Run Yale E-mail*, YALE DAILY NEWS (Feb. 9, 2010), <http://www.yaledailynews.com/news/university-news/2010/02/09/google-run-yale-e-mail/>.

¹⁶⁵ The law should be strengthened to protect users merely at the mercy of Google’s “Don’t be Evil” motto and to ensure that Google cannot currently volunteer whatever data it wants to government or private entities.

¹⁶⁶ See *supra* Part I. The presence of a monopoly is a factor in determining whether or not a violation of a plaintiff’s Fourteenth Amendment rights has occurred in situations where court access is limited. See *Boddie v. Conn.*, 401 U.S. 371, 375 (1971). By analogy, a service provider’s monopoly over a user’s constitutional rights might be an effective bar to justice, violating their due process and equal protection rights.

collection activities and the prospects of a third party such as Google voluntarily handing over data to the government.¹⁶⁷ Under current law, the most likely remedy for affected telecommunication or Internet service users are lawsuits against companies for breaching their own privacy policies. However, as discussed, such terms are often ambiguous and confer no definite rights upon a user.

In *United States v. Bach*, the U.S. Court of Appeals for the Eighth Circuit held that Yahoo!'s execution of a search warrant to retrieve a user's email was not unreasonable under the Fourth Amendment. Instead, the court noted that civilian searches at times might be more reasonable than law enforcement searches.¹⁶⁸ The *Bach* case and existing Fourth Amendment analogies make clear that Internet Service Providers (ISP) should be liable as a state actor when they execute a search warrant on behalf of law enforcement.¹⁶⁹ Absent an exception, a company should not disclose information in which an individual has an objectively reasonable subjective expectation of privacy unless a warrant has been issued or an exception has been met, and no such warrant shall issue without probable cause. However, it is unclear as to whether or not a private actor is restricted as a state actor when it is not executing a search warrant.

The U.S. Court of Appeals for the Fourth Circuit recently rejected the notion that a private email host should be restricted by the Fourth Amendment when it provides information to the government without a law enforcement request. In *Richardson*, a defendant sought unsuccessfully to suppress evidence against him that was initially detected and retrieved by AOL and eventually turned over to law enforcement.¹⁷⁰ He argued that AOL effectively was deputized by a federal law mandating that service providers report evidence of child pornography.¹⁷¹ Therefore, AOL was required to comply with Fourth Amendment

¹⁶⁷ This is no longer a hypothetical in light of Google's recent decision to voluntarily provide information to the NSA in exchange for help in thwarting cyber attacks. See Ellen Nakashima, *Google to Enlist NSA to Help it Ward off Cyberattacks*, WASH. POST, Feb. 4, 2010, <http://www.washingtonpost.com/wp-dyn/content/article/2010/02/03/AR2010020304057.html>.

¹⁶⁸ 310 F.3d 1063, 1067 (8th Cir. 2002).

¹⁶⁹ Francisco J. Navarro, *United States v. Bach and the Fourth Amendment in Cyberspace*, 14 ALB. L.J. SCI. & TECH. 245, 263–265 (2003).

¹⁷⁰ See *United States v. Richardson*, 607 F.3d 357, 360 (4th Cir. 2010).

¹⁷¹ *Id.* at 367.

2011] The Fourth Amendment in the Age of Google 185

restrictions and utilize an automated search system to detect and extract illegal photos from his email.¹⁷² The court rejected this concept and noted that the federal law did not require ISPs to conduct searches nor did it dictate the means by which they should execute them.¹⁷³ Thus, AOL's search was a voluntary private party action not subject to Fourth Amendment restrictions despite the fact that it later turned over information to the government in fulfillment of the statute's reporting requirements.¹⁷⁴

In other cases, foreign private parties have hacked illegally into a computer, stole files, and turned them over to the government which used the evidence to initiate cases and prosecute individuals.¹⁷⁵ In these cases, the Fourth Amendment was not applied even though the hackers essentially acted as agents of law enforcement. Therefore, it is necessary to examine the state action doctrine to determine how it should apply to third parties, which lack personalities but boast more advanced technical knowhow and surveillance capabilities than law enforcement agencies.

B. The State Action Doctrine

Constitutional restraints on third parties only apply when state action is attached to third party actions.¹⁷⁶ Otherwise, users enjoy merely the statutory protections afforded to electronic data. The Fourth Amendment is a restriction on the government and does not explicitly bar a private party from searching or seizing a person's property. Moreover, Fourth Amendment jurisprudence has not always recognized restraints on private actors who illegally seize property from an individual and later turn it over to the government.¹⁷⁷ In the 1921 case of *Burdeau v. McDowell*, the U.S. Supreme Court held that such an action, while perhaps theft, did not trigger the Fourth Amendment even when the government refused to return the property.¹⁷⁸ However, this clear bright line private-public

¹⁷² *Id.* at 362–63.

¹⁷³ *Id.* at 366–67.

¹⁷⁴ *Id.*

¹⁷⁵ See Sagi Schwartzberg, *Hacking the Fourth: How the Gaps in the Law and Fourth Amendment Jurisprudence Leave the Right to Privacy at Risk*, 30 U. LA VERNE L. REV. 467, 484–86 (2009).

¹⁷⁶ *Burdeau v. McDowell*, 256 U.S. 465, 470–71, 475 (1921).

¹⁷⁷ *Id.* at 476.

¹⁷⁸ *Id.*

constitutional rights distinction eroded in 1974 with the U.S. Supreme Court case of *Jackson v. Metropolitan Edison Co.*¹⁷⁹

In *Jackson*, the Court outlined a state action test to determine whether or not a private actor was acting as a state actor and thus could be restricted on constitutional grounds. From this precedent and subsequent case law, the Court has allowed constitutional limitations on private actors engaging in the exercise of “powers traditionally exclusively reserved to the State.”¹⁸⁰ This initial exception allowing for constitutional restraints on private actors required both the traditional role and the exclusive role criteria to be met for the Court to accept a private actor as a *de facto* state actor. However, in today’s dynamic world new technologies are replacing traditional functions, such as mail delivery, with expansive communication platforms not contemplated by traditional notions of exclusive state functions.

In *Jackson*, Metropolitan Edison was a private utility company which operated under a state-sanctioned license in a service area in the state of Pennsylvania.¹⁸¹ The company was regulated under the Pennsylvania Public Utility Commission and vested with the authority to disconnect customers who did not pay.¹⁸² Petitioner Catherine Jackson was a customer of Metropolitan Edison and her electricity was disconnected as a result of her failure to pay. She subsequently sued under the Civil Rights Act of 1871 on the grounds that Metropolitan Edison violated her Fourteenth Amendment due process rights by neglecting to give her sufficient notice, a hearing, and an opportunity to repay debts.¹⁸³ This lawsuit was based on the petitioner’s insistence that Metropolitan Edison’s actions constituted “state action” by virtue of its state-granted power to disconnect electricity for non-payment.¹⁸⁴ The state-granted power came from the company’s operating agreement with the Commission.¹⁸⁵

¹⁷⁹ *Jackson v. Metro. Edison Co.*, 419 U.S. 345, 346, 350 (1974).

¹⁸⁰ *Id.* at 346, 352. Communication service providers have some functions that mimic traditional state functions such as postal delivery. Letters, photos, and documents are increasingly sent digitally via private actors rather than through the government run service. However, these functions, have not traditionally been exclusive to the state due to the existence of private parcel carriers such as UPS and FedEx or even the short-lived Pony Express.

¹⁸¹ *Id.* at 346.

¹⁸² *Id.*

¹⁸³ *Id.* at 347–48.

¹⁸⁴ *Id.* at 348–49.

¹⁸⁵ *Id.* at 348.

2011] The Fourth Amendment in the Age of Google 187

Writing for the Court, Justice William Rehnquist acknowledged that the distinction between a private action and a state action “frequently admits of no easy answer.”¹⁸⁶ The due process clause of the Fourteenth Amendment places restraints on state actors’ abilities to deprive the life, liberty, and property of an individual without due process of law. The Court stated that regulation alone does not make the actions of a private entity those of the state.¹⁸⁷ However, the opinion noted that the actions of a “governmentally protected monopoly” might more likely be considered state actions.¹⁸⁸ Justice Rehnquist wrote that the determination of state action did not rest on how state-like the actor was but instead on how closely the action was linked to the state.¹⁸⁹

The Court reiterated that utility services, though perhaps a public function, never have been regarded as an exercise of a traditional state power, such as eminent domain.¹⁹⁰ The Court also made clear that monopoly status alone did not subject a private entity to the Fourteenth Amendment.¹⁹¹ Therefore, a plaintiff suing a private actor for a constitutional violation would have to show more than evidence of heavy regulation and a partial monopoly to prove state action.¹⁹² Additionally, the mere fact that a private actor exercises a behavior permitted under the law does not mean that a state action has occurred.¹⁹³ Ultimately, the Court asked, “[W]hether there is a sufficiently close nexus between the State and the challenged action of the regulated entity so that the action of the latter may be fairly treated as that of the State itself.”¹⁹⁴ Although state action was not found in *Jackson*, the Court set a precedent for plaintiffs to enforce their constitutional rights against private actors when the actions are so closely linked to those of the state.

C. Post-Jackson and Rethinking the State Action Doctrine

Since *Jackson*, the Court has expanded the doctrine to allow for lawsuits against private entities that do not fulfill the rigid

¹⁸⁶ *Id.* at 346, 349–50.

¹⁸⁷ *Id.* at 349–50.

¹⁸⁸ *Id.* at 350–51.

¹⁸⁹ *Id.* at 351.

¹⁹⁰ *Id.* at 353.

¹⁹¹ *Id.* at 352.

¹⁹² *Id.* at 358.

¹⁹³ *Id.* at 357.

¹⁹⁴ *Id.* at 351.

public function test.¹⁹⁵ However, the most relevant application of the state action doctrine to the current public-private information sharing dilemma comes from the 2001 case, *Brentwood Academy v. Tennessee Secondary School Athletic Association*.¹⁹⁶ In *Brentwood*, the Court articulated the entwinement exception to the state action doctrine, holding that a private athletic organization which regulated the athletics programs of public and private schools in the state was constitutionally restricted in its actions against the plaintiff because of its “entwinement” with the state.¹⁹⁷

The decision permitted the plaintiff to sue the athletics association for violating its First and Fourteenth Amendment rights, despite the fact that there was no legal requirement for schools to join the private entity. The Court cited the factors of overt and covert “encouragement” by the state as criteria when weighing the entwinement.¹⁹⁸ One of the determinative factors in *Brentwood* was the state’s appointment of public officials to the board of the private entity.¹⁹⁹ Likewise, in the past decade communication providers have assigned employees to work onsite with the FBI to provide calling information for quick “sneak peek” inquiries.²⁰⁰ Such an arrangement would appear to be evidence of an “entwinement” of the government with a private entity, at least for these specific types of searches.²⁰¹ If the concept of “entwinement” was applied more broadly to law enforcement methods then constitutional restrictions might govern private searches that effectively moot the need of the government to conduct a search. One instance would be if a

¹⁹⁵ See generally, Henry C. Strickland, *The State Action Doctrine and the Rehnquist Court*, 18 HASTINGS CONST. L.Q. 587 (1991) (discussing the evolution of the State Action Doctrine since the Civil Rights Cases).

¹⁹⁶ *Brentwood Acad. v. Tenn. Secondary Sch. Athletic Ass’n*, 531 U.S. 288 (2001).

¹⁹⁷ *Id.* at 290–91.

¹⁹⁸ *Id.* at 296 (holding a plaintiff is allowed to sue for a deprivation of property without due process of law claim when a private party acted at the encouragement of the state (citing *Lugar v. Edmondson Oil Co.*, 457 US 922, 941 (1982))).

¹⁹⁹ *Id.* at 291, 300.

²⁰⁰ OVERSIGHT AND REVIEW DIV., U.S. DEP’T OF JUSTICE OFFICE OF THE INSP’R GEN., A REVIEW OF THE FEDERAL BUREAU OF INVESTIGATION’S USE OF EXIGENT LETTERS AND OTHER INFORMAL REQUESTS FOR TELEPHONE RECORDS 72 (Jan. 2010), available at <http://www.justice.gov/oig/special/s1001r.pdf>.

²⁰¹ *United States v. Attson*, 900 F.2d 1427, 1429 (9th Cir. 1990) (“[T]he fourth amendment [sic] will only apply to governmental conduct that can reasonably be characterized as a ‘search’ or a ‘seizure.’”).

2011] The Fourth Amendment in the Age of Google 189

communication service provider such as Google, actively scanned private data for national security or criminal activity and then voluntarily handed it over to the government.

A requirement necessary to apply the state action doctrine to the Fourth Amendment is that the information itself is actually protected. For example, the U.S. Court of Appeals for the Fifth Circuit refused to apply the state action doctrine when the information retrieved by a private actor acting on behalf of the FBI yielded insurance records that would be uncovered in the course of a normal audit.²⁰² Thus, this logic would apply to information possessed by a communication service provider in which users have no expectations of privacy. However, encrypted, password-protected data stored in a user's account likely would not be exposed during the course of a normal audit.

The U.S. Court of Appeals for the Ninth Circuit created a more easily satisfied two part test to determine whether a private party could be restrained under the Fourth Amendment, asking: "(1) whether the government knew of and acquiesced in the intrusive conduct, and (2) whether the party performing the search intended to assist law enforcement efforts or to further his own ends."²⁰³ If applied to the programs similar to the NSA Terrorist Surveillance Program, then collusive companies likely would be restricted as a state actor under this test. Additionally, the aforementioned volunteer hacker-vigilante scenarios conceivably could satisfy both prongs. Moreover, this test could safeguard adequately the rights of users of Google's Gmail and similar services and prevent them from becoming the backbone of a warrantless digital dragnet.

The state action doctrine is one possible avenue by which a person can enforce Fourth Amendment protections against third parties. The incredible surveillance powers possessed by communication providers exceed, replace, and complement the exclusive traditional powers of law enforcement entities. Therefore, this concept should be applied along with factors of entwinement and the Ninth Circuit's two prong test to determine whether or not private searches are state actions. The Fourth Amendment should restrain private searches by communication service providers when content-data is turned over to the government.

²⁰² *United States v. Blocker*, 104 F.3d 720, 727 (5th Cir. 1997).

²⁰³ *United States v. Miller*, 688 F.2d 652, 657 (9th Cir. 1982).

VIII. CONCLUSION

The Fourth Amendment must be applied to online communications to withstand and adapt to modern citizen behavior. The voluntary and secret disclosure of personal user information by third party telecommunication companies during the NSA Warrantless Surveillance incident demonstrates the potential privacy implications for citizens entrusting storage of their documents and effects to cloud computing companies. Hackers and private parties are a much greater threat to information security than the law enforcement regimes of democratically elected governments. However, as public-private partnerships increase out of necessity, constitutional protections should follow so that traditional rights are not evaded by way of outsourcing digital searches to volunteer private entities.

Left unrestricted, private entities might build erroneous character profiles improperly targeting innocent people due to trigger words used in online documents or web searches. The goal of Internet-era Fourth Amendment jurisprudence must not be to thwart investigations but rather to prevent fishing expeditions. It is important not to impede the efforts of law enforcement officials to solve crimes or prevent terrorist attacks. For this, a digital false friend exists. Law enforcement officials can still retrieve instant messages, emails, and shared documents from the person in whom the suspect confides or through the traditional warrant process. Undercover agents still can befriend suspects or laypersons online as a means of following and developing investigative leads. Moreover, online data still can be accessed without prior notice for national security investigations utilizing the FISA regime.

Citizens should enjoy a reasonable expectation of privacy from unwarranted government intrusion in their password-protected digital documents and effects repositories even in the cloud. Federal courts should distinguish the traditional third party doctrine analogy from the anonymous and automated role played by a communication service provider. Moreover, the state action doctrine should be expanded to permit constitutional rights to restrict searches conducted by communication service providers. This would prevent TOS agreements from trumping reasonable expectations of privacy. In the mean time, Congress should update the Electronic Communication Privacy Act to protect and recognize the digital documents and effects that have functionally replicated and replaced those mentioned in the text

2011] The Fourth Amendment in the Age of Google 191

of the Fourth Amendment.

The stakes of not adapting the protections of the Fourth Amendment to modern realities will increase as interconnected databases, cross-referencing technologies, and the prevalence of cloud computing expand. Future research should examine the potential national security problems posed if foreign companies purchase domestic communication service providers and obtain access to the vast amounts of data held by American corporations and regulated by American laws. Export controls placed on the sale of the data itself or even restrictions on server locations should be examined in light of the legal and privacy implications of recent hacking incidents and the privacy expectations analyzed in this research. Ultimately, legal regimes must continue to evolve with technology to reduce uncertainty and ambiguity for citizens and service providers alike.


2012

The Mosaic Theory of the Fourth Amendment

Orin S. Kerr

George Washington University Law School

Follow this and additional works at: <http://repository.law.umich.edu/mlr>

 Part of the [Fourth Amendment Commons](#), [Law Enforcement and Corrections Commons](#), [Science and Technology Law Commons](#), and the [Supreme Court of the United States Commons](#)

Recommended Citation

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

Available at: <http://repository.law.umich.edu/mlr/vol111/iss3/1>

This Article is brought to you for free and open access by the Michigan Law Review at University of Michigan Law School Scholarship Repository. It has been accepted for inclusion in Michigan Law Review by an authorized editor of University of Michigan Law School Scholarship Repository. For more information, please contact mlaw.repository@umich.edu.

THE MOSAIC THEORY OF THE FOURTH AMENDMENT

Orin S. Kerr*

In the Supreme Court's recent decision on GPS surveillance, United States v. Jones, five justices authored or joined concurring opinions that applied a new approach to interpreting Fourth Amendment protection. Before Jones, Fourth Amendment decisions had always evaluated each step of an investigation individually. Jones introduced what we might call a "mosaic theory" of the Fourth Amendment, by which courts evaluate a collective sequence of government activity as an aggregated whole to consider whether the sequence amounts to a search.

This Article considers the implications of a mosaic theory of the Fourth Amendment. It explores the choices and puzzles that a mosaic theory would raise, and it analyzes the merits of the proposed new method of Fourth Amendment analysis. The Article makes three major points. First, the mosaic theory represents a dramatic departure from the basic building block of existing Fourth Amendment doctrine. Second, adopting the mosaic theory would require courts to answer a long list of novel and challenging questions. Third, courts should reject the theory and retain the traditional sequential approach to Fourth Amendment analysis. The mosaic approach reflects legitimate concerns, but implementing it would be exceedingly difficult in light of rapid technological change. Courts can better respond to the concerns animating the mosaic theory within the traditional parameters of the sequential approach to Fourth Amendment analysis.

TABLE OF CONTENTS

INTRODUCTION	312
I. THE SEQUENTIAL APPROACH TO THE FOURTH AMENDMENT	315
A. <i>Sequential Analysis in Search and Seizure Law</i>	315
B. <i>The Search Inquiry Under the Sequential Approach</i>	316
C. <i>Constitutional Reasonableness Under the Sequential Approach</i>	317
D. <i>Constitutional Remedies Under the Sequential Approach</i>	319
II. MAYNARD/JONES AND THE INTRODUCTION OF THE MOSAIC THEORY	320
A. <i>The Facts of Maynard/Jones</i>	321
B. <i>The D.C. Circuit's Opinion the Maynard</i>	323
C. <i>The Supreme Court's Opinions in Jones</i>	326
III. IMPLEMENTING THE MOSAIC THEORY	328

* Fred C. Stevenson Research Professor, George Washington University Law School. Thanks to Will Baude, David Pozen, Daniel Solove, Paul Ohm, Marc Blitz, and Steve Leckar for comments on an earlier draft.

A. <i>Identifying the Standard</i>	330
1. Expectations of What?	330
2. The Stages of Surveillance	331
B. <i>The Grouping Problem: Developing a Theory of Aggregation for the Mosaic Search</i>	333
1. Duration and Scale	333
2. Which Surveillance Methods Count?	334
3. Grouping Across Practices, Officers, and Investigations	335
C. <i>The Constitutional Reasonableness of Mosaic Searches</i>	336
D. <i>Remedies for Mosaic Searches</i>	340
1. Does the Exclusionary Rule Apply?	340
2. Standing to Challenge Mosaic Searches	342
3. Fruit of the Poisonous Tree and Inevitable Discovery	343
IV. THE CASE AGAINST THE MOSAIC THEORY	343
A. <i>The Mosaic Theory as Equilibrium-Adjustment</i>	345
B. <i>The Case Against the Mosaic Theory</i>	346
1. The Mosaic Theory Would Be Very Difficult to Administer	346
2. Probabilistic Approaches to the "Reasonable Expectation of Privacy" Test Are Ill Suited to Regulate Technological Surveillance	348
3. The Mosaic Theory Could Interfere with More Effective Statutory Protections	350
C. <i>The Mosaic Theory as a Halfway Measure and the Katz Example</i>	352
CONCLUSION	353

INTRODUCTION

The Fourth Amendment prohibits unreasonable searches and seizures,¹ and the most challenging and important threshold question in interpreting the Fourth Amendment is what counts as a "search."² Identifying Fourth Amendment searches traditionally has required analyzing police action sequentially.³ If no individual step in a sequence counts as a search, then the Fourth Amendment is not triggered. No Fourth Amendment violation has occurred.

1. U.S. CONST. amend. IV.

2. The issue of what counts as a seizure is comparatively simple, and it therefore has received little scholarly attention. Seizures require governmental assertion of control, so a seizure of property occurs when the government meaningfully interferes with a person's possessory interest. *United States v. Jacobsen*, 466 U.S. 109, 113 (1984).

3. See *infra* Section I.A.

In *United States v. Maynard*,⁴ the D.C. Circuit introduced a different approach, which could be called a “mosaic theory” of the Fourth Amendment.⁵ Under the mosaic theory, searches can be analyzed as a collective sequence of steps rather than as individual steps.⁶ Identifying Fourth Amendment searches requires analyzing police actions over time as a collective “mosaic” of surveillance; the mosaic can count as a collective Fourth Amendment search even though the individual steps taken in isolation do not.⁷ The D.C. Circuit applied that test in *Maynard* to GPS surveillance of a car. The court held that GPS surveillance of a car’s location over twenty-eight days aggregates into so much surveillance that the collective sequence triggers Fourth Amendment protection.⁸

When the Supreme Court reviewed *Maynard* in *United States v. Jones*,⁹ concurring opinions signed or joined by five of the justices endorsed some form of the D.C. Circuit’s mosaic theory.¹⁰ The majority opinion resolved the case without reaching the mosaic theory, and neither concurring opinion gave the issue extensive analysis. But Justice Alito’s concurring opinion for four justices clearly echoed the basic reasoning of the D.C. Circuit in concluding that long-term GPS monitoring of a car counts as a search even though short-term monitoring does not.¹¹ Justice Sotomayor’s separate concurrence also voiced support for the mosaic approach.¹²

The concurring opinions in *Jones* raise the intriguing possibility that a five-justice majority of the Supreme Court is ready to endorse a new mosaic theory of Fourth Amendment protection. That prospect invites lower courts to consider whether the mosaic theory is viable and if so, how it should be applied. A handful of courts have begun to do so in the short time since the Court handed down *Jones*, with mixed results so far.¹³ Law enforcement is

4. 615 F.3d 544 (D.C. Cir.), *aff’d sub nom.* *United States v. Jones*, 132 S. Ct. 945 (2012).

5. I first used this label in a blog post published on the day the *Maynard* decision was handed down. See Orin Kerr, *D.C. Circuit Introduces “Mosaic Theory” of Fourth Amendment, Holds GPS Monitoring a Fourth Amendment Search*, VOLOKH CONSPIRACY (Aug. 6, 2010, 2:46 PM), <http://volokh.com/2010/08/06/d-c-circuit-introduces-mosaic-theory-of-fourth-amendment-holds-gps-monitoring-a-fourth-amendment-search/>. Other labels are possible, but for the sake of consistency I will adhere to that term.

6. *Maynard*, 615 F.3d at 562 n.*.

7. *Id.* at 566.

8. *Id.* at 561–62.

9. 132 S. Ct. 945.

10. See *infra* Section II.C.

11. *Jones*, 132 S. Ct. at 963–64 (Alito, J., concurring in the judgment). Justice Alito’s opinion was joined by Justices Ginsburg, Breyer, and Kagan.

12. *Id.* at 956 (Sotomayor, J., concurring) (reasoning that determining whether government behavior constitutes a search requires considering “whether people reasonably expect that their movements will be recorded and aggregated” in such a manner).

13. Compare *United States v. Graham*, 846 F. Supp. 2d 384 (D. Md. 2012) (rejecting the mosaic theory for collection of cell-site data), with *Mont. State Fund v. Simms*, 270 P.3d 64, 69–72 (Mont. 2012) (Nelson, J., specially concurring) (suggesting that the mosaic theory should apply to public camera surveillance).

paying close attention as well. Soon after *Jones*, the General Counsel of the Federal Bureau of Investigation informed a law school audience that the mosaic opinions in *Jones* were causing significant turmoil inside the FBI.¹⁴

The mosaic opinions in *Jones* implicate fundamental questions about the future of Fourth Amendment law. What might a mosaic theory mean? What challenges does it entail? Should lower courts eagerly adopt such a method, or do its risks outweigh its benefits? And when the mosaic theory eventually works its way back up to the Supreme Court, should the Court embrace it as a valid theory or reject it as misguided?

This Article considers the consequences of possible judicial adoption of a mosaic theory. It maps out the possible futures of the mosaic theory, and it details how the theory raises questions that courts will need to answer.¹⁵ It also evaluates the merits of the mosaic approach and considers whether judges should accept the invitation to adopt it.

The Article makes three points. First, the mosaic theory is a major departure from the traditional mode of Fourth Amendment analysis. The current structure of Fourth Amendment doctrine hinges on what I call a “sequential approach.” The sequential approach takes a snapshot of each discrete step and assesses whether that discrete step at that discrete time constitutes a search. This analytical method forms the foundation of existing Fourth Amendment doctrine, ranging from the threshold question of what the Fourth Amendment regulates to considerations of constitutional reasonableness and remedies. By aggregating conduct rather than looking to discrete steps, the mosaic theory offers a fundamental challenge to current Fourth Amendment law.

Second, implementing the mosaic theory would require courts to answer an extensive list of difficult and novel questions. Severing the Fourth Amendment from the sequential approach would compel courts to start afresh with a new building block of Fourth Amendment analysis. For example, what is the standard for the mosaic? How should courts aggregate conduct to know when a sufficient mosaic has been created? Which techniques should fall within the mosaic approach? Should mosaic searches require a warrant? If so, how can mosaic warrants satisfy the particularity requirement? Should the exclusionary rule apply to violations of the mosaic search doctrine? Who has standing to challenge mosaic searches? Adopting

14. See Ariane de Vogue, *Supreme Court Ruling Prompts FBI to Turn Off 3,000 Tracking Devices*, YAHOO! NEWS (Mar. 7, 2012), <http://news.yahoo.com/supreme-court-ruling-prompts-fbi-turn-off-3-154046722--abc-news.html>.

15. A few student notes and online journal articles have touched on the mosaic theory in the wake of *Maynard*, although none have addressed its operation and merits in detail. Examples include Priscilla J. Smith et al., *When Machines Are Watching: How Warrantless Use of GPS Surveillance Technology Violates the Fourth Amendment Right Against Unreasonable Searches*, 121 YALE L.J. ONLINE 177, 201 (2011), <http://yalelawjournal.org/images/pdfs/1017.pdf>; Erin Smith Dennis, Note, *A Mosaic Shield: Maynard, the Fourth Amendment, and Privacy Rights in the Digital Age*, 33 CARDOZO L. REV. 737 (2011); Justin P. Webb, Note, *Carving Out Notions of Privacy: The Impact of GPS Tracking and Why Maynard Is a Move in the Right Direction*, 95 MARQ. L. REV. 751 (2011–12).

a mosaic theory would require courts to answer all of these questions and more.

Third, as a normative matter, courts should reject the mosaic theory. The mosaic approach is animated by legitimate concerns: it aims to maintain the balance of Fourth Amendment protection as technology changes, a method I have elsewhere called “equilibrium-adjustment.”¹⁶ But it aims to achieve this reasonable goal in a peculiar way. By rejecting the building block of the sequential approach, the mosaic theory would be very difficult to administer coherently. Even if courts could develop answers to the many questions the theory raises, doing so would take many years—by which time the technologies regulated by the theory would become obsolete. The mosaic theory would also deter enactment of statutory privacy regulations and force judges to consider questions that they are poorly equipped to answer. If courts must broaden Fourth Amendment rules in response to new technologies, the better approach is to rule that certain steps are always searches. The model should be the Supreme Court’s famous decision in *Katz v. United States*,¹⁷ not the concurring opinions in *Jones*.

This Article proceeds in four parts. Part I introduces the sequential approach that forms the basis for existing Fourth Amendment doctrine. Part II provides a close analysis of the D.C. Circuit and Supreme Court decisions on the mosaic theory in *Maynard* and *Jones*. Part III catalogs and considers the many difficult issues that courts would need to answer to implement the mosaic theory. Finally, Part IV argues that courts should reject the mosaic theory and retain the traditional sequential approach to interpreting the Fourth Amendment.

I. THE SEQUENTIAL APPROACH TO THE FOURTH AMENDMENT

This Section explains how the sequential approach to Fourth Amendment analysis forms the building block of modern Fourth Amendment doctrine. It begins by introducing the sequential approach and then examines the three basic stages of Fourth Amendment analysis: first, what is a search; second, when is a search unreasonable and therefore unconstitutional; and third, when does an unconstitutional search justify a remedy.

A. Sequential Analysis in Search and Seizure Law

Fourth Amendment analysis traditionally has followed what I call the sequential approach: to analyze whether government action constitutes a Fourth Amendment search or seizure, courts take a snapshot of the act and assess it in isolation. The “step-by-step analysis is inherent”¹⁸ in evaluating Fourth Amendment claims. This does not mean that searches or seizures happen

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

17. 389 U.S. 347 (1967).

18. *United States v. Beaudoin*, 362 F.3d 60, 70–71 (1st Cir. 2004), *vacated sub nom. Champagne v. United States*, 125 S. Ct. 1025 (2005) (mem.).

instantaneously. An officer might search a home for a few hours and then seize evidence found inside for the duration of the investigation. But analyzing whether a search has occurred requires a frame-by-frame dissection of the scene. As the Supreme Court has explained, courts focus on each "particular governmental invasion of a citizen's personal security,"¹⁹ starting with the "initial" step and then separately analyzing the "subsequent" steps.²⁰

Consider a few examples. If an officer inserts a key into the door of a residence and then opens the door to enter, a reviewing court will first consider the act of inserting the key and then analyze the distinct act of opening the door.²¹ If an officer sees expensive stereo equipment in an apartment, moves it to see the serial number, and then records the serial number, a court will treat moving the equipment as distinct from recording the number.²² If an officer sees suspects preparing for a robbery, stops them, and pats them down for weapons, the court will consider the viewing, the stopping, and the patting down as distinct acts that must be analyzed separately.²³ Each step counts as its own Fourth Amendment event and is evaluated independently of the others.

The sequential approach is not merely a minor aspect of Fourth Amendment doctrine. Rather, it forms the foundation of existing search and seizure analysis. The remainder of this Section explains how the basic structure of existing Fourth Amendment law rests on the sequential approach. It starts with the threshold question of defining a search, then turns to constitutional reasonableness, and concludes with Fourth Amendment remedies.

B. *The Search Inquiry Under the Sequential Approach*

The Supreme Court's established methods for identifying when a Fourth Amendment search occurs reflects the sequential approach. From the 1960s until the Court's recent *Jones* case, the search inquiry was governed by the "reasonable expectation of privacy" test introduced in Justice Harlan's famous concurring opinion in *Katz*.²⁴ Although the phrase "reasonable expectation of privacy" is notoriously murky, much of the Supreme Court's case law on the reasonable expectation of privacy test can be understood as distinguishing between inside and outside surveillance. Conduct violates a reasonable expectation of privacy when a government actor breaks into a private, enclosed

19. *Terry v. Ohio*, 392 U.S. 1, 19 (1968).

20. *See United States v. Dionisio*, 410 U.S. 1, 8-9 (1973).

21. *E.g.*, *United States v. Moses*, 540 F.3d 263, 272 (4th Cir. 2008).

22. *Arizona v. Hicks*, 480 U.S. 321, 324-25 (1987).

23. *See Terry*, 392 U.S. at 18 n.15, 27-30.

24. *See Smith v. Maryland*, 442 U.S. 735, 739-40 (1979). The Supreme Court's decision in *United States v. Jones* explains that this is not the only test, *see* 132 S. Ct. 945, 953-54 (2012), but proponents of the mosaic theory have rooted it solely in this test.

space,²⁵ such as a home,²⁶ a car,²⁷ a package,²⁸ or a person's pockets.²⁹ The entrance into the private space exposes the contents of the private space, and the search occurs at the moment of exposure.³⁰ In contrast, conduct does not violate a reasonable expectation of privacy when it consists of observing the outside of property,³¹ observing what has already been exposed to the public,³² or observing public spaces where anyone may travel.³³

The sequential approach forms the basic unit of analysis under this traditional inquiry. To know if a search has occurred, courts ask if the government's conduct has crossed the boundary from outside to inside surveillance. So long as the government has stayed outside and acquired no information about what is inside, no search has occurred.³⁴ A search only happens when the police learn about what is hidden inside a private space, whether by squeezing a duffle bag to learn its contents³⁵ or aiming a thermal imaging device at a home to learn its temperature.³⁶

The sequential approach also applies to the trespass test revived in *Jones*. Under *Jones*, a Fourth Amendment search occurs when government actors trespass onto persons, houses, papers, or effects with intent to obtain information.³⁷ The sequential approach naturally matches this traditional doctrine. A search occurs at the moment of the trespass, and it lasts for the period of the trespass. Identifying when a search occurs therefore requires analyzing the government conduct frame by frame and asking when the conduct triggers a trespass.

C. Constitutional Reasonableness Under the Sequential Approach

The sequential approach also forms a basic part of the next inquiry: whether searches are constitutionally reasonable. Over time, the Supreme

25. See, e.g., *Silverman v. United States*, 365 U.S. 505, 511 (1961) ("At the very core [of the Fourth Amendment] stands the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion.").

26. *Id.*

27. *United States v. Ross*, 456 U.S. 798, 807–09, 823–25 (1982).

28. E.g., *United States v. Jacobsen*, 466 U.S. 109, 114 (1984).

29. *Minnesota v. Dickerson*, 508 U.S. 366, 378 (1993).

30. See *United States v. Karo*, 468 U.S. 705, 712 (1984) ("[W]e have never held that potential, as opposed to actual, invasions of privacy constitute searches for purposes of the Fourth Amendment. . . . It is the exploitation of technological advances that implicates the Fourth Amendment, not their mere existence.").

31. *New York v. Class*, 475 U.S. 106, 114 (1986).

32. *Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring) (stating that "objects, activities, or statements" that a person "exposes to the 'plain view' of outsiders" do not receive Fourth Amendment protection).

33. See *Kyllo v. United States*, 533 U.S. 27, 32 (2001).

34. See, e.g., *United States v. Knotts*, 460 U.S. 276, 281–82 (1983).

35. See *Bond v. United States*, 529 U.S. 334, 336–37 (2000).

36. *Kyllo*, 533 U.S. at 34–35.

37. *United States v. Jones*, 132 S. Ct. 945, 951 n.5 (2012).

Court has offered two different approaches to the reasonableness of searches. In the middle of the twentieth century, the Court generally indicated that searches are reasonable only when the government obtains a valid warrant or a special exception to the warrant requirement applies.³⁸ More recently, the Court has suggested a different approach. Reasonableness now is understood as requiring a balancing of interests: courts consider whether the government interests advanced by the use of an investigatory technique outweigh the privacy interests that its use threatens.³⁹ Under this approach, reasonableness may require a warrant but may require less regulation or even no regulation at all.⁴⁰

Both approaches to reasonableness rest on the assumption that searches are readily identifiable acts that occur over readily identifiable periods of time.⁴¹ This allows courts to balance the interests for specific kinds of searches and create categories for when different searches are reasonable. A few examples demonstrate the point. Under existing Supreme Court precedent, searching a home ordinarily requires a warrant.⁴² In contrast, searching a car implicates a different balancing of interests and leads to a different

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

39. *See, e.g.*, *United States v. Place*, 462 U.S. 696, 703 (1983) ("We must balance the nature and quality of the intrusion on the individual's Fourth Amendment interests against the importance of the governmental interests alleged to justify the intrusion.").

40. For example, the Court in *Samson v. California* explained the balancing approach as follows:

"[U]nder our general Fourth Amendment approach" we "examin[e] the totality of the circumstances" to determine whether a search is reasonable within the meaning of the Fourth Amendment. Whether a search is reasonable "is determined by assessing, on the one hand, the degree to which it intrudes upon an individual's privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests."

547 U.S. 843, 848 (2006) (alterations in original) (citations omitted) (quoting *United States v. Knights*, 534 U.S. 112, 118-19 (2001)).

41. It is true that searches and seizures both occur over a period of time, and the reasonableness inquiry must be made over that period of time. For example, if an officer enters a home and searches for one hour while a second officer detains the homeowner for two hours, the search will occur for one hour while the seizure will last for two hours. But the fact that searches and seizures occur over time does not mean that they reject the sequential approach or implicate a "mosaic." Their existence and duration are clear as they occur, and do not require the ex post aggregation and analysis of non-searches.

42. In *United States v. Karo*, the Court stated as follows:

At the risk of belaboring the obvious, private residences are places in which the individual normally expects privacy free of governmental intrusion not authorized by a warrant, and that expectation is plainly one that society is prepared to recognize as justifiable. Our cases have not deviated from this basic Fourth Amendment principle. Searches and seizures inside a home without a warrant are presumptively unreasonable absent exigent circumstances.

468 U.S. 705, 714-15 (1984).

rule: because cars are less private than homes, searching a car requires probable cause but no warrant.⁴³ A pat-down frisk for weapons implicates yet another balancing. The need to protect officers' safety alters the balance so that the police need only specific and articulable facts that a person is armed and dangerous in order to conduct the frisk.⁴⁴

Special rules apply in special circumstances as well. For example, the government's need to protect the federal border enables federal agents to routinely search a person and his property at the border or its functional equivalent.⁴⁵ The need to stop terror attacks allows the Transportation Security Administration ("TSA") to screen individuals and their property at the airport without suspicion.⁴⁶ On the other hand, particularly intrusive searches receive heightened protection. For example, the police cannot search a person's body to retrieve evidence if that intrusion might threaten the person's health, even if they have a warrant.⁴⁷ In each of these cases, the analysis presupposes that a search is a readily identifiable act that allows courts to analyze the strength of the interests in play when the government commits that kind of act.

The sequential approach also forms the foundation for the warrant requirement. The purpose of the warrant requirement is to ban unlimited searches that allow investigators to go anywhere and search for any kind of evidence.⁴⁸ To curb this abuse, the Warrant Clause includes a particularity requirement: warrants must "particularly describ[e] the place to be searched, and the persons or things to be seized."⁴⁹ The particularity requirement limits searches by requiring them to occur in a particular place and to look for specific evidence, such as a search of 123 Main Street for marijuana.⁵⁰ Here the sequential approach has obvious force: the particularity requirement rests on the premise that searches are identifiable acts that occur in identifiable places to find identifiable evidence.

D. Constitutional Remedies Under the Sequential Approach

Fourth Amendment law also reflects a sequential method of analysis at the remedies stage. Consider the causation principles generally required for Fourth Amendment liability. Remedies apply only if the unconstitutional act caused the discovery of a specific piece of evidence.⁵¹ Establishing causation requires examining two questions. First, was the unconstitutional act a

43. See *California v. Carney*, 471 U.S. 386, 392–94 (1985).

44. See *Terry v. Ohio*, 392 U.S. 1, 31 (1968).

45. See *United States v. Flores-Montano*, 541 U.S. 149, 152–53 (2004).

46. See *Elec. Privacy Info. Ctr. v. U.S. Dep't of Homeland Sec.*, 653 F.3d 1, 10–11 (D.C. Cir.), *reh'g en banc denied*, 653 F.3d 1 (D.C. Cir. 2011).

47. See *Winston v. Lee*, 470 U.S. 753, 766 (1985).

48. See *Maryland v. Garrison*, 480 U.S. 79, 84 (1987).

49. U.S. CONST. amend. IV.

50. See *Garrison*, 480 U.S. at 84.

51. See *Hudson v. Michigan*, 547 U.S. 586, 590–94 (2006).

"but for" cause of the discovery of the evidence? Second, was the unconstitutional act a proximate cause of the discovery of the evidence? In the context of the exclusionary rule, the "but for" causation test consists of the "inevitable discovery" and "independent source" doctrines. The proximate cause inquiry takes the form of the colorfully labeled "fruit of the poisonous tree" doctrine.⁵² Similar concepts govern remedies in the context of civil damages, although courts use the traditional labels of causation analysis.⁵³

This causal analysis is naturally tailored to the sequential approach. Deciding whether an influence caused a particular result requires a specific definition of the influence. Identifying whether a particular fact counts as a proximate cause of a result requires identifying the specific fact, which then permits an evaluation of how much that fact contributed to the result. The same is true with the Fourth Amendment's standing inquiry, which requires the defendant who seeks relief to show that his own rights were violated.⁵⁴ Establishing standing generally requires pointing to a particular act in a particular time and place that counts as a search. Courts can then determine if the movant had a sufficient connection to the place searched at that time to establish standing.⁵⁵

II. *MAYNARD/JONES* AND THE INTRODUCTION OF THE MOSAIC THEORY

The mosaic theory poses a fundamental challenge to the sequential approach. The theory first arose in a recent case, *United States v. Maynard*,⁵⁶ later reviewed by the Supreme Court under the name *United States v. Jones*.⁵⁷ The mosaic theory requires courts to apply the Fourth Amendment search doctrine to government conduct as a collective whole rather than in isolated steps. Instead of asking if a particular act is a search, the mosaic theory asks whether a series of acts that are not searches in isolation amount to a search when considered as a group. The mosaic theory is therefore premised on aggregation: it considers whether a set of nonsearches aggregated together amount to a search because their collection and subsequent analysis creates a revealing mosaic.

Understanding the new mosaic theory must begin with a close study of *Maynard/Jones* at both the D.C. Circuit and Supreme Court levels. A close reading of *Maynard/Jones* suggests that five justices are ready to embrace the new mosaic approach to the Fourth Amendment: Justices Ginsburg, Breyer,

52. See *Wong Sun v. United States*, 371 U.S. 471, 484–88 (1963).

53. In the civil setting, courts have used similar concepts but under traditional causation labels such as intervening causes and events that break the chain of causation. See, e.g., *Hector v. Watt*, 235 F.3d 154, 160–61 (3d Cir. 2000).

54. See *Rakas v. Illinois*, 439 U.S. 128, 133–34 (1978). Although *Rakas* warns that the label "standing" is inaccurate, it remains a convenient and widely used shorthand.

55. See *id.*

56. 615 F.3d 544 (D.C. Cir. 2010).

57. 132 S. Ct. 945 (2012).

Alito, Kagan, and Sotomayor.⁵⁸ The next Section analyzes *Maynard/Jones* with an eye toward understanding how the analysis in *Maynard/Jones* shifted the framework for analyzing Fourth Amendment searches from the sequential approach to the mosaic theory. It then considers what the mosaic theory might mean for the future of Fourth Amendment law.

A. The Facts of *Maynard/Jones*

Antoine Jones owned a nightclub in Washington, D.C.⁵⁹ Lawrence Maynard served as the nightclub's manager.⁶⁰ In 2004, a joint federal and local narcotics task force began to suspect Jones and Maynard of orchestrating a massive conspiracy to sell cocaine and crack.⁶¹ A complex two-year investigation followed and ultimately led to the discovery of 97 kilograms of cocaine, 1 kilogram of crack, and \$850,000 in cash in a stash house run by Jones and Maynard.⁶²

Investigators used a wide range of techniques to develop the case against Jones and Maynard. They obtained wiretap orders and pen register orders to monitor the suspects' telephones,⁶³ and they relied on informants to share tips about the conspiracy.⁶⁴ They also installed a camera at the front door of the nightclub to watch who entered and left.⁶⁵ Additionally, investigators obtained search warrants to collect copies of text messages shared among the suspects.⁶⁶

The investigators also used a range of techniques to identify the targets' location. Sophisticated drug dealers generally structure their conspiracies to keep higher-level members away from the contraband.⁶⁷ That way, if the police swoop in, they will find and arrest only low-level dealers who are easy to replace.⁶⁸ As leaders of the conspiracy, Jones and Maynard stayed as far away from the drugs as possible. Investigators therefore used three different methods to monitor the physical location of both Jones and Maynard to try to tie them to the conspiracy. The first method of identifying the location

58. *Jones*, 132 S. Ct. at 963–64 (Alito, J., concurring in the judgment); *id.* at 956 (Sotomayor, J., concurring).

59. *Maynard*, 615 F.3d at 549.

60. *Id.*

61. *Id.*

62. *See Jones*, 132 S. Ct. at 948–49.

63. *United States v. Jones*, 451 F. Supp. 2d 71, 74 (D.D.C. 2006), *aff'd in part, rev'd in part sub nom. 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).

64. *Id.*

65. *Jones*, 132 S. Ct. at 948.

66. *Jones*, 451 F. Supp. 2d at 74.

67. This may be familiar to fans of the television series *The Wire* (HBO television broadcast).

68. *See id.*

of Jones and Maynard was very traditional: the investigators put Jones and Maynard under visual surveillance.⁶⁹

The second method was more sophisticated. The police knew Jones's cell phone number. Cell phones work by connecting to local cell towers, which route communications. Because cell phone providers routinely keep records of which towers were used by each account, the government can obtain cell phone records that act as a rough kind of location device. Most people carry their phones: the location of a suspect's phone tells the police the location of the suspect. In *Maynard/Jones*, investigators applied for and obtained court orders requiring Jones's cellular provider to provide cell tower information (called "cell-site" data) for Jones's phone.⁷⁰ The government obtained several court orders pursuant to the Stored Communications Act⁷¹ and collected four months' worth of records logging the location of the phone. The government did not seek admission of this evidence at trial, however.⁷²

The appellate decisions in *Maynard/Jones* focused on the third method of location monitoring: use of a GPS device installed on Jones's car. Jones drove a Jeep Grand Cherokee that belonged to his wife.⁷³ Officers obtained a warrant from a judge in the District of Columbia authorizing them to install a GPS device on the car.⁷⁴ At the time, no legal authority indicated that a warrant was necessary. Although precedents were sparse, and the D.C. courts had not spoken on the issue, other federal courts had ruled that the Fourth Amendment did not apply in such circumstances.⁷⁵ The agents obtained a warrant nonetheless, perhaps recognizing that the Supreme Court had not yet settled the issue.⁷⁶ Having proceeded cautiously in light of legal uncertainty, however, the agents then blundered in executing the warrant. The warrant required officers to install the device inside the District of Columbia within ten days of the warrant's issuance. The agents did not install the GPS device until the eleventh day when the car happened to be at a public parking lot in Maryland.⁷⁷

69. *Jones*, 132 S. Ct. at 948.

70. See Defendant's Motion to Suppress Cell Site Data & Memorandum of Points & Authorities in Support Thereof at 1-3, *United States v. Jones*, No. 05-CR-386(1) (ESH) (D.D.C. Mar. 29, 2012) [hereinafter Defendant's Motion to Suppress], available at http://legaltimes.typepad.com/files/jones_gps.pdf.

71. See 18 U.S.C. § 2703(d) (2006) (permitting noncontent records from cellular phones to be obtained based on an application establishing specific and articulable facts).

72. Following the Supreme Court ruling, however, the prosecution is presently attempting to retry Jones in the district court using the cell-site data. See Defendant's Motion to Suppress, *supra* note 70, at 4.

73. *Jones*, 132 S. Ct. at 948.

74. *Id.*

75. See, e.g., *United States v. McIver*, 186 F.3d 1119, 1126-27 (9th Cir. 1999), *abrogated by Jones*, 132 S. Ct. 945.

76. Cf. *People v. Weaver*, 909 N.E.2d 1195, 1203 (N.Y. 2009) (holding that placement and use of a GPS device on a car is a "search" under the New York State constitution).

77. *Jones*, 132 S. Ct. at 948.

The officers used the GPS device to record the location of Jones's car for twenty-eight days. The battery-powered GPS device could record the location of the car within approximately 50 to 100 feet.⁷⁸ Whenever the car was in motion, the GPS device used cell phone technology to broadcast signals of the car's location to a government computer every seven seconds. The device produced over 2,000 pages of location data over twenty-eight days. The location information helped show that Jones's movements were coordinated with those of his co-conspirators, and that he would rendezvous with his co-conspirators and visit the stash house in Fort Washington, Maryland, where the drugs and cash were later found.⁷⁹

At trial, the prosecution attempted to admit the GPS evidence to show that Jones was involved in the conspiracy. Jones moved to suppress the GPS evidence. Judge Ellen Huvelle agreed with Jones that any evidence indicating that the car was inside Jones's garage had been obtained in violation of the Fourth Amendment.⁸⁰ However, Judge Huvelle concluded that the remaining GPS evidence was admissible under *United States v. Knotts*.⁸¹ *Knotts* had permitted the use of a radio beeper located in a car that broadcasted the car's location to the police nearby. According to the Supreme Court in *Knotts*, using the radio beeper to follow the location of a car on public roads did not violate any reasonable expectation of privacy:

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.⁸²

Judge Huvelle reasoned that the same analysis applied to monitoring using a GPS device.⁸³ Maynard pled guilty, but Jones went to trial. The jury convicted Jones in a retrial after the first trial resulted in a hung jury.⁸⁴

B. The D.C. Circuit's Opinion in Maynard

Maynard and Jones appealed their convictions, although only Jones challenged the GPS evidence used to convict him at trial. Jones argued on appeal that *Knotts* was distinguishable because a GPS device was "light

78. *Id.*

79. *See id.* at 948–49.

80. *United States v. Jones*, 451 F. Supp. 2d 71, 88 (D.D.C. 2006), *aff'd in part, rev'd in part sub nom. 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).

81. 460 U.S. 276 (1983).

82. *Knotts*, 460 U.S. at 281–82.

83. *Jones*, 451 F. Supp. 2d at 88.

84. *Jones*, 132 S. Ct. at 948–49.

years away”⁸⁵ from a radio beeper. Far from merely enhancing the senses, the GPS device could gather so much evidence over time that it could create a full picture of a person’s life. Quoting a law student note published in the *Boston College Law Review*,⁸⁶ Jones argued that GPS monitoring was so intrusive, even in public, that it resembled an invasive search:

Even though one may expect fleeting glances in public, and police should not have to avert their eyes from what they can see in public, one does not thereby expect the targeted aggregation of data a GPS device collects on one’s movements, particularly a kind of surveillance the individual can neither detect nor prevent.⁸⁷

The D.C. Circuit affirmed Maynard’s conviction but reversed Jones’s conviction on the ground that use of the GPS device over twenty-eight days was a Fourth Amendment search.⁸⁸ Judge Douglas Ginsburg reasoned that *Knotts* was inapplicable because *Knotts* had suggested that “dragnet-type law enforcement practices” might trigger “different constitutional principles.”⁸⁹ They did, Judge Ginsburg reasoned, and installing and monitoring a GPS device was one such dragnet-type practice. *Knotts* therefore did not control.

Once freed from *Knotts*, Judge Ginsburg turned to the “reasonable expectation of privacy” inquiry. Judge Ginsburg relied on a string of cases applying what I have elsewhere called the probabilistic model of Fourth Amendment protection.⁹⁰ Under these cases, whether government conduct violates a reasonable expectation of privacy depends in significant part on the likelihood that evidence will be exposed to the public.⁹¹ In Judge Ginsburg’s view, these cases indicated that the core question raised by GPS monitoring was the likelihood that the information collected by GPS monitoring was exposed to the public.⁹²

Judge Ginsburg’s answer to this question redefined the basic unit of Fourth Amendment law. Instead of looking at the likelihood that discrete pieces of GPS information would be exposed to the public, Judge Ginsburg considered whether the entirety of the GPS monitoring over the course of twenty-eight days, *considered as a collective whole*, would be so exposed.

85. See Brief for Appellants at 54, *United States v. Maynard*, 615 F.3d 544 (D.C. Cir. 2010) (No. 08-3030), 2009 WL 3155141.

86. April A. Otterberg, *GPS Tracking Technology: The Case for Revisiting Knotts and Shifting the Supreme Court’s Theory of the Public Space Under the Fourth Amendment*, 46 B.C. L. REV. 661 (2005).

87. See Brief for Appellants, *supra* note 85, at 60 (quoting Otterberg, *supra* note 86, at 696–97).

88. *United States v. Maynard*, 615 F.3d 544, 568 (D.C. Cir. 2010), *aff’d sub nom. United States v. Jones*, 132 S. Ct. 945 (2012).

89. *Id.* at 556–58 (citing *United States v. Knotts*, 460 U.S. 276, 283–84 (1983)).

90. See Orin S. Kerr, *Four Models of Fourth Amendment Protection*, 60 STAN. L. REV. 503, 508–12 (2007).

91. *Id.*

92. *Maynard*, 615 F.3d at 558.

In his view, the monitoring over time constituted a “search” because it was extremely unlikely that the public would actually observe the entirety of such movements.⁹³ Members of the public would surely see discrete parts of Jones’s movements considered in isolation. But it was essentially impossible for any one person to observe the complete set:

[T]he whole of a person’s movements over the course of a month is not actually exposed to the public because the likelihood a stranger would observe all those movements is not just remote, it is essentially nil. It is one thing for a passerby to observe or even to follow someone during a single journey as he goes to the market or returns home from work. It is another thing entirely for that stranger to pick up the scent again the next day and the day after that, week in and week out, dogging his prey until he has identified all the places, people, amusements, and chores that make up that person’s hitherto private routine.⁹⁴

Judge Ginsburg acknowledged that the discrete readings of the GPS device revealed information exposed to the public. But he reasoned that even if each of the individual readings were exposed in a constructive sense—that is, exposed even if no one actually observed them—the collective entity of the twenty-eight days of surveillance was not so exposed. This was true because the collective sum of twenty-eight days of surveillance revealed more than the sum of its parts. “The difference is not one of degree but of kind,” Judge Ginsburg wrote, “for 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.”⁹⁵ Many nonsearches packaged together as a collective entity *became* a search because the individual pieces of the puzzle that seemed small in isolation could be assembled together like a mosaic to reveal the full picture of a person’s life.

For precedent, Judge Ginsburg turned to a Freedom of Information Act case, *U.S. Department of Justice v. Reporters Committee for Freedom of the Press*.⁹⁶ *Reporters Committee* held that the FBI had properly refused to disclose “rap sheets” listing the criminal convictions of individuals under an exception to FOIA that applies when the disclosure could reasonably be expected to constitute an invasion of personal privacy.⁹⁷ Although individual acts reported on the rap sheets were already public, the Supreme Court reasoned that bringing the information together for easy access made a major difference: “Plainly there is a vast difference between the public records that might be found after a diligent search of courthouse files, county archives, and local police stations throughout the country and a computerized summary located in a single clearinghouse of information.”⁹⁸

93. *Id.*

94. *Id.* at 560.

95. *Id.* at 562.

96. 489 U.S. 749 (1989).

97. *Reporters Committee*, 489 U.S. at 779–80.

98. *Id.* at 764.

Judge Ginsburg argued that the same mosaic principle should apply in the Fourth Amendment setting. The whole was not merely the sum of its parts:

Prolonged surveillance reveals types of information not revealed by short-term surveillance, such as what a person does repeatedly, what he does not do, and what he does ensemble. These types of information can each reveal more about a person than does any individual trip viewed in isolation. Repeated visits to a church, a gym, a bar, or a bookie tell a story not told by any single visit, as does one's not visiting any of these places over the course of a month. The sequence of a person's movements can reveal still more; a single trip to a gynecologist's office tells little about a woman, but that trip followed a few weeks later by a visit to a baby supply store tells a different story. A person who knows all of another's travels can deduce whether he is a weekly church goer, a heavy drinker, a regular at the gym, an unfaithful husband, an outpatient receiving medical treatment, an associate of particular individuals or political groups—and not just one such fact about a person, but all such facts.⁹⁹

When considered as a collective whole, the monitoring over twenty-eight days was a Fourth Amendment search because it revealed “an intimate picture of the subject’s life that he expects no one to have—short perhaps of his spouse.”¹⁰⁰ The D.C. Circuit denied rehearing over several dissents, including one by Judge Kavanaugh that pointed to an alternative rationale: perhaps the installation of the device, rather than its use, constituted the search.¹⁰¹

C. The Supreme Court’s Opinions in Jones

The Supreme Court unanimously agreed that Jones had been the subject of a Fourth Amendment search but divided sharply on why.¹⁰² Writing for a five-justice majority, Justice Scalia followed Judge Kavanaugh’s suggestion and held that the installation of the GPS device was a search because it was a trespass on the “effects” of the car.¹⁰³ Having resolved the case on trespass grounds, Justice Scalia did not need to reach the mosaic theory adopted in the D.C. Circuit.¹⁰⁴ However, five justices wrote or joined opinions that did touch on the mosaic theory. Their opinions are somewhat cryptic, but they suggest that a majority of the Court is ready to embrace some form of the D.C. Circuit’s mosaic theory.

The first opinion to consider is Justice Alito’s concurrence in the judgment. Justice Alito wrote for four justices, as his opinion was joined by

99. *Maynard*, 615 F.3d at 562.

100. *Id.* at 563.

101. See *United States v. Jones*, 625 F.3d 766, 769–71 (D.C. Cir. 2010) (Kavanaugh, J., dissenting), *denying reh’g en banc* to *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).

102. See *United States v. Jones*, 132 S. Ct. 945 (2012).

103. *Id.* at 951–54.

104. *Id.* at 953–54.

Justices Ginsburg, Breyer, and Kagan.¹⁰⁵ Most of Justice Alito's opinion criticized the majority's trespass rationale.¹⁰⁶ Near the end, however, his opinion turned to how he would have resolved the case under the reasonable expectation of privacy test.¹⁰⁷ Justice Alito accepted *United States v. Knotts* but construed it as limited to "relatively short-term monitoring of a person's movements."¹⁰⁸ According to Justice Alito, the long-term monitoring of the car presented a different issue.¹⁰⁹

Justice Alito applied the reasonable expectation of privacy test by invoking expectations of how law enforcement investigate particular crimes. According to Justice Alito, society has an expectation as to how different offenses might be investigated. For most offenses, "society's expectation has been that law enforcement agents and others would not—and indeed, in the main, could not"¹¹⁰ monitor the location of the suspect's car in the detailed way GPS monitoring enabled. The same might not be true of an "extraordinary offense[],"¹¹¹ Justice Alito suggested. For "extraordinary" crimes, such extensive monitoring might be expected based on "previously available techniques."¹¹² But because the conspiracy in *Jones* was not, in Justice Alito's view, "extraordinary," the degree of observation implicated by long-term monitoring exceeded society's expectations and therefore constituted a Fourth Amendment search.

Justice Alito's analysis is cryptic, in part because this section of his opinion cites no authority. At the same time, his opinion echoes the D.C. Circuit's mosaic approach in *Maynard*. Like the D.C. Circuit, Justice Alito concluded that long-term GPS monitoring constituted a search while short-term monitoring did not.¹¹³ More broadly, by shifting the probabilistic inquiry from what a person might expect the public to *see* to what a person might expect the police to *do*, Justice Alito introduced the element of time, which is critical to the mosaic approach. Justice Alito analyzed the constitutionality of the monitoring in *Jones* by asking if the entirety of the monitoring over twenty-eight days exceeded societal expectations. Implicitly, the unit of the search was a collective whole over an extended period of time.

The fifth justice to touch on the mosaic theory was Justice Sotomayor. Justice Sotomayor joined the majority opinion and also agreed with Justice Alito that use of a GPS device constituted a search, independent of its installation. Justice Sotomayor reasoned that "the unique attributes of GPS

105. *Id.* at 957–64 (Alito, J., concurring in the judgment).

106. *Id.* at 958–62.

107. *Id.* at 963–64.

108. *Id.* at 964.

109. *Id.*

110. *Id.*

111. *See id.*

112. *Id.*

113. *Id.*

monitoring"¹¹⁴—its precision, detail, and efficiency—should guide the constitutional analysis of its use:

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.¹¹⁵

This passage clearly echoes the mosaic theory. Justice Sotomayor focuses on whether a person has Fourth Amendment rights "in the sum" of their public movements, rather than in individual movements. Second, Justice Sotomayor asks whether people reasonably expect that their movements not only will be recorded but also "aggregated." This is the language of sums from the mosaic theory, not the language of individual acts from the sequential approach.

Importantly, Justice Sotomayor's version of the mosaic theory suggests a different standard than that adopted by Justice Alito. Justice Alito's opinion focused on surprise. It looked to whether the investigation exceeded society's expectations for how the police would investigate a particular crime.¹¹⁶ In contrast, Justice Sotomayor's approach looked to whether police conduct collected so much information that it enabled the government to learn about a person's private affairs "more or less at will."¹¹⁷ Despite these differences, both of the concurring opinions in *Jones* analyze the collective sum of government action, rather than individual sequential steps, to determine what counts as a Fourth Amendment search.

III. IMPLEMENTING THE MOSAIC THEORY

The possible adoption of the mosaic theory raises challenging new questions for the future of Fourth Amendment law. It is undoubtedly true that combining many pieces of information about suspects can lead the government to learn intimate details about their lives.¹¹⁸ In the past, however, this was considered good police work rather than cause for alarm. The repeated use of nonsearch techniques has been considered an essential way to create probable cause that justifies searches rather than an unlawful search itself.¹¹⁹

114. *Id.* at 955 (Sotomayor, J., concurring).

115. *Id.* at 956.

116. *See id.* at 964 (Alito, J., concurring in the judgment).

117. *See id.* at 955–56 (Sotomayor, J., concurring).

118. *See, e.g.,* David E. Pozen, *Deep Secrecy*, 62 STAN. L. REV. 257, 284 (2010) ("As more and more items of information emerge about a secret plan or policy, outsiders will have more and more opportunities to draw inferences across the items and to relate them to other items of information they possess. Such analytic mosaic-making is a basic precept of intelligence gathering, used by our government to learn about our enemies and by our enemies to learn about us.").

119. *Cf. United States v. R. Enters., Inc.*, 498 U.S. 292, 297 (1991) ("[T]he Government cannot be required to justify the issuance of a grand jury subpoena by presenting evidence

The very different premises of the mosaic theory open a wide range of new questions for courts to answer.

This Section analyzes the choices that courts must consider if they decide to adopt a mosaic approach. The lesson of this Section is that implementing a mosaic theory would require courts to answer a remarkable set of novel and difficult questions. The theory is so different from what has come before that implementing it would require the creation of a parallel set of Fourth Amendment rules. For every settled question of law under the sequential approach, courts would need to reanalyze the framework under the mosaic theory. And, for the most part, the mosaic version would be exponentially more complicated. Under the sequential approach, searches are simple points. Replacing those points with complex aggregates over space and time is akin to introducing *Flatland's* square to a three-dimensional world.¹²⁰

The analysis focuses on four major questions:

1. *The Standard Question.* The first question concerns the standard that would govern the mosaic theory. What test determines when a mosaic has been created? The three pro-mosaic opinions in *Maynard/Jones* suggested three different standards, and future courts will have to choose which standard to adopt. Articulating the standard also requires determining what stages of surveillance a mosaic search regulates. Is data collection enough, or is subsequent analysis and use also required? If the latter, what are the constitutional standards for data analysis and disclosure?
2. *The Grouping Question.* If courts adopt a mosaic theory, they will need a theory of grouping to explain how conduct should be grouped to assess whether the collective whole crosses the mosaic line. The mosaic theory groups conduct that is not a search and asks if the nonsearches considered together cross the line to become a search. This requires courts to answer a series of grouping questions. Which surveillance methods prompt a mosaic approach? Should courts group across surveillance methods? If so, how? What is the half-life of a mosaic search?
3. *Constitutional Reasonableness.* The next question is how to analyze the reasonableness of mosaic searches. Mosaic searches do not fit an obvious doctrinal box for determining reasonableness. The nature of the mosaic is that each mosaic will be different, potentially requiring different kinds of reasonableness analyses for each one. This concern is bolstered by the fact that the mosaic may aggregate across many different kinds of surveillance, each of which will raise its own reasonableness concerns. Courts will therefore have to create a framework for determining the reasonableness of mosaic searches.
4. *Remedies for Mosaic Violations.* The final question concerns what remedies should apply to unconstitutional mosaic searches. Does the

sufficient to establish probable cause because the very purpose of requesting the information is to ascertain whether probable cause exists.”).

120. EDWIN A. ABBOTT, *FLATLAND: A ROMANCE OF MANY DIMENSIONS* (5th ed., Harper & Row 1963) (1884).

exclusionary rule apply? If so, does the rule extend over all of the mosaic or only the surveillance that crossed the line to trigger a search? Who has standing to challenge mosaic searches? How should courts apply remedial limitations such as inevitable discovery given that only parts of the mosaic may have been inevitably discovered? Also, when should civil remedies be available for mosaic theory violations? Courts will have to craft a new remedial jurisprudence for the new mosaic search doctrine.

A. Identifying the Standard

The first challenge raised by the potential adoption of a mosaic theory is selecting the proper standard for aggregation. This question divides into two parts. The first requires identifying the proper reference point for when a mosaic has been created. The second requires choosing which stages of surveillance the mosaic theory regulates: initial data collection, subsequent analysis, or both.

1. Expectations of What?

The first question raised by the mosaic theory is what kinds of expectations of privacy the mosaic theory should recognize. The three pro-mosaic opinions in *Maynard/Jones* each suggest a different answer. Justice Alito focused on societal expectations about law enforcement practices.¹²¹ In his view, a search occurs when investigators collect and analyze evidence in a way or to a degree that would surprise members of society.¹²² In contrast, Justice Sotomayor offered a more normative standard that looked at government power. In her view, a search occurs when the government can learn details about a person's personal life "more or less at will."¹²³ In the D.C. Circuit opinion introducing the mosaic theory, Judge Ginsburg offered yet another standard, focusing on whether the government learned more than a stranger could have observed. These approaches are quite different. If courts adopt the mosaic theory, which version should they use?

Choosing among the different versions of the mosaic theory is particularly difficult because each formulation contains major ambiguities. Consider Justice Alito's approach, which focuses on societal beliefs about police powers.¹²⁴ Applying Alito's standard requires courts first to identify what a reasonable person thinks about existing police investigations and then to identify when an investigation exceeds that expectation in some measured way. This is a difficult task. Objective standards are used widely within Fourth Amendment law. But most people lack direct experience with police investigations. As a result, they have little basis on which to estimate what is common or uncommon about particular investigations. Even among

121. See *Jones*, 132 S. Ct. at 964 (Alito, J., concurring in the judgment).

122. *Id.*

123. *Id.* at 956 (Sotomayor, J., concurring).

124. *Id.* at 964 (Alito, J., concurring in the judgment).

experienced officers, reasonable estimates will diverge. Different agencies investigate different cases in different circumstances in different ways.

Given the public's poor understanding of police practices and the wide variation among those practices, it is unclear what courts are supposed to measure or how they are supposed to measure it.¹²⁵ Nor is it clear what kind of deviations from that expectation can trigger the mosaic. Investigations can involve many people using many tools over time. Any reasonably competent defense attorney can find at least some aspect of an investigation that might surprise a member of the public in some way. Implementing Justice Alito's approach therefore requires courts to develop a theory of which deviations matter and how much.

Justice Sotomayor's approach is even more ambiguous than Justice Alito's. According to Justice Sotomayor, courts must 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."¹²⁶ If taken literally, this language appears to direct courts to first identify a threshold of "more or less at will" for how easily the government can "record and aggregate" information about a person's "political and religious beliefs, sexual habits, and so on." Courts must then determine whether the public has the reasonable expectations that this will occur. But what does this mean? Phrases like "and so on" and "more or less at will" do not identify legal standards as much as make suggestions for further inquiry. Adopting Justice Sotomayor's standard would require significant elaboration.

Ambiguities remain if courts use Judge Ginsburg's standard and look to the likelihood that private actors would conduct similar surveillance. What do courts know about the kinds of surveillance practices that businesses, marketers, and private investigators might conduct? How similar is similar enough? Is the relevant standard whether the aggregation of evidence exceeds societal expectations of what one single stranger would see, or what all strangers collectively would see? Adopting Judge Ginsburg's standard would require courts to answer such questions.

2. The Stages of Surveillance

The next question is what stages of surveillance the mosaic theory would regulate. Surveillance regimes often involve several stages: first, the acquisition of information; second, the analysis of that information; and third, the use or disclosure of that information.¹²⁷ Fourth Amendment law traditionally has focused only on the first step—the acquisition of information.¹²⁸ The

125. I develop this point further *infra* in Section IV.B.2.

126. *Jones*, 132 S. Ct. at 956 (Sotomayor, J., concurring).

127. Orin S. Kerr, *Use Restrictions and the Future of Surveillance Law* 4–5 (Brookings Inst. The Future of the Constitution Series, 2011), available at http://www.brookings.edu/~media/research/files/papers/2011/4/19%20surveillance%20laws%20kerr/0419_surveillance_law_kerr.pdf.

128. *Id.* at 6, 9–10.

subsequent analysis and use of information has been considered beyond the scope of Fourth Amendment protection.¹²⁹

The mosaic theory could change this. Justice Alito's opinion in *Jones* looked to whether a person reasonably expects others to "secretly monitor and catalog"¹³⁰ a person's movements. Justice Sotomayor asked "whether people reasonably expect that their movements will be recorded and aggregated"¹³¹ in a manner that creates the mosaic. Cataloging and aggregating are verbs that describe subsequent analysis instead of initial collection. These phrases suggest that the mosaic theory requires some step beyond the acquisition stage.

If so, courts will need to determine what kinds of postacquisition conduct are required to create a mosaic. Imagine the government collects a great deal of information but never combines it into a single database. Has a mosaic been created? Or imagine the evidence is collected into a database but never analyzed. Does that cross the line? If some analysis of the evidence is required to trigger the mosaic, what kind of analysis counts? Does any analysis suffice, or is there some threshold of sophistication or computational complexity before the mosaic line has been crossed?

Identifying the precise stage regulated by the mosaic theory is particularly important in light of the requirement of state action in Fourth Amendment law. The Fourth Amendment only applies to conduct by the government or its agents.¹³² If private parties conduct surveillance, that surveillance cannot constitute a Fourth Amendment search unless the parties acted as agents of the government.¹³³ The state action requirement raises difficult questions because government agents and private parties can divide surveillance tasks. To see the problem, imagine that a private party collects mosaic data without government involvement. Now imagine that the government obtains a court order compelling the private party to disclose it, or that the private party voluntarily discloses the records to the government. Government investigators then analyze the data and use it to identify a suspect's whereabouts or conduct. Does the Fourth Amendment apply if a private party created the data and the government only analyzed it? And what if the roles are reversed, and the government collects the data that is then analyzed by a private party? Does the Fourth Amendment apply to the collection without analysis? Shifting from a sequential approach to a mosaic theory

129. This is true for two reasons. First, if the information collected is not subject to Fourth Amendment protection, then its analysis raises no Fourth Amendment issues. *See, e.g., State v. Sloane*, 939 A.2d 796, 797 (N.J. 2008) (holding that searching through a database of criminal records is not a Fourth Amendment "search" because the criminal records are matters of public record). Second, even if the information collected was once subject to Fourth Amendment protection, the initial search of that information eliminates a subsequent expectation of privacy. *See Illinois v. Andreas*, 463 U.S. 765, 771 (1983) ("[O]nce police are lawfully in a position to observe an item firsthand, its owner's privacy interest in that item is lost.").

130. *Jones*, 132 S. Ct. at 964 (Alito, J., concurring in the judgment) (emphasis added).

131. *Id.* at 956 (Sotomayor, J., concurring) (emphasis added).

132. *United States v. Jacobsen*, 466 U.S. 109, 113-14 (1984).

133. *See id.*

requires identifying exactly which steps in the mosaic require government action to trigger Fourth Amendment protections.

*B. The Grouping Problem: Developing a Theory of
Aggregation for the Mosaic Search*

After courts settle on a standard to gauge if a mosaic has been created, the next question is how to solve the grouping problem. The mosaic theory looks at an aggregated set of data acquisitions, and it determines when they trigger a collective search. Applying this approach requires a theory of grouping—a theory of what should be aggregated and how—to assess when that trigger point has been reached. Three kinds of questions must be considered: first, duration and how to measure scale; second, which surveillance methods count; and third, how and whether to group across different investigations.

1. Duration and Scale

The first initial grouping question is the most obvious: how long must the tool be used before the relevant mosaic is created? In *Jones*, the GPS device was installed for twenty-eight days. Justice Alito stated that this was “surely”¹³⁴ long enough to create a mosaic. But he provided no reason why, and he recognized that “other cases may present more difficult questions.”¹³⁵ If twenty-eight days is too far, how about fourteen days? Or 3.6 days? Where is the line?

Identifying the length of time only scratches the surface of the problem. 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?

Software can be configured to collect data in more complex ways, further complicating the problem. Imagine the GPS device is set to record the location of the car only once a month, precisely at midnight on the first day of each month. If the police install the device and use it for one month, they will have only one data point. Should this count as one month of location monitoring? Or is it only a single observation? In the language of Justice Alito’s opinion, is this “long-term” surveillance that triggers a search or “short-term” surveillance that does not? What if the device records once a day or once a week instead of only once a month?

134. *Jones*, 132 S. Ct. at 964 (Alito, J., concurring in the judgment) (“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.”).

135. *Id.*

A related question is whether delay makes a difference. Does a mosaic have a half-life, such that the portion of an earlier mosaic fades over time and restarts the mosaic clock? Assume, for the sake of argument, that the Supreme Court eventually draws the line for continuous GPS monitoring at seven days. When the monitoring has occurred for seven days, a search has occurred. Now imagine that the police monitor a suspect for five days and then give up and remove the GPS device. A few years later, the police decide to reopen the case, and they install another GPS device and use it for three days. Does this count as eight days of monitoring, such that the mosaic was created and the conduct was a search? Or does this count as five days of monitoring in one year and three days of monitoring a few years later, neither of which is a search?¹³⁶

The counting problem is exacerbated by the fact that different suspects will act differently at different times. The amount of private information collected by the surveillance will vary greatly from suspect to suspect. For example, imagine the police know that one suspect rarely uses his car while a second suspect drives several hours a day. The police install GPS devices on both cars for one week, revealing very little about the first suspect and a great deal about the habits of the second. Does the mosaic amount to a search earlier for the second suspect than for the first? Or do the days of monitoring accumulate in the same way regardless of how the car is used? Does it matter if the police know these differences before the monitoring occurs? Courts will have to decide whether these differences matter, and if so, if they matter independently of police knowledge or if some police knowledge is required.

2. Which Surveillance Methods Count?

The next set of questions considers which surveillance methods trigger the mosaic theory and whether and how to group across different methods. The facts of *Maynard/Jones* are illustrative. In *Maynard/Jones*, GPS surveillance was only one tool among many that investigators used. The government obtained cell phone location records, installed a public surveillance camera, and watched the suspects in public, all in addition to tapping phones and obtaining text messages.¹³⁷ When considering whether conduct amounts to a mosaic, which of these different tools are subject to the mosaic inquiry?

Consider a few examples, starting with surveillance methods that monitor location. Should the mosaic theory apply to obtaining records for cell-site location transmitted from the suspect's phone to the suspect's service provid-

136. An additional complication is that a group of coconspirators can share a group of cars, and each car can have a surveillance device installed for different periods of time. See, e.g., *United States v. Luna-Santillanes*, No. 11-20492, 2012 WL 1019601, at *6-7 (E.D. Mich. Mar. 26, 2012) (considering mosaic arguments in a case involving a conspiracy of three narcotics defendants who drove three cars, each of which had a GPS device installed for different periods of time).

137. See *supra* notes 62-71.

er?¹³⁸ Should the theory apply if the government uses a drone (an unmanned aerial surveillance vehicle) to monitor the location of the suspect's car? Or cameras that read license plates? If the police send a team of investigators to place the suspect under visual surveillance, should that visual surveillance be subject to the same analysis? How about public camera surveillance, such as that created by closed-circuit television cameras or by government investigators monitoring suspects in public?¹³⁹ Any of these technologies can be used to identify a suspect's location over time. If courts adopt the mosaic approach, they will need to answer whether the mosaic theory applies to these techniques.

The next question is whether the mosaic theory only applies to location surveillance. The GPS device in *Jones* broadcast the location of Jones's car, and the collective record of the location of the car over time allowed the government to assemble a picture of what Jones did during that period. But many surveillance tools can assemble a picture of a suspect's life without revealing the person's location. The police might collect records containing every email address a suspect wrote to and every telephone number a suspect dialed. Investigators might monitor the IP address of every website that a suspect visited. They might obtain a suspect's credit card statements showing purchases the suspect made over many months. If the mosaic theory applies to location monitoring, courts will need to consider whether the same theory extends to other kinds of surveillance.

If the mosaic theory applies to multiple surveillance methods, courts must also consider whether the duration and scale questions raised earlier should be answered in the same way for every method. Different methods of surveillance have different levels of invasiveness. As a result, different methods of surveillance might require different regulation within the mosaic framework. If the mosaic approach applies to cell-site surveillance, for example, should the required period of surveillance to trigger a search be longer than the period for GPS surveillance because cell-site surveillance is less exact and invasive than GPS surveillance? Or should all techniques subject to a mosaic analysis be treated in the same way?

3. Grouping Across Practices, Officers, and Investigations

If the mosaic approach applies to multiple surveillance practices, the next question is whether and how to group across them. In *Maynard/Jones*, the police simultaneously monitored a suspect using cell-site tracking, visual surveillance, and GPS monitoring.¹⁴⁰ If the mosaic theory applies to each surveillance method individually, should courts apply the theory to each surveillance method in isolation? Or should they ask whether the collective of

138. See, e.g., *United States v. Graham*, 846 F. Supp. 2d 384 (D. Md. 2012) (rejecting the mosaic theory for collection of cell-site data).

139. See, e.g., *Mont. State Fund v. Simms*, 270 P.3d 64, 69–72 (Mont. 2012) (Nelson, J., specially concurring) (suggesting that the mosaic theory should apply to public camera surveillance).

140. See *supra* notes 62–73.

some or all of these methods amounts to a search?¹⁴¹ If seven days of continuous GPS monitoring creates a mosaic search, how should courts treat, say, six days of combined monitoring through GPS together with three days of cell-site monitoring and one day of visual monitoring? Does that count as ten days' worth of monitoring, or only six?

Because multiple investigations can target the same suspect, courts may need to consider whether the mosaic aggregates across different investigations. Imagine a suspect is under investigation by both federal and state authorities. After the suspect buys a car that has a GPS device installed on it, the state investigators turn on the GPS device. They monitor the suspect for five days and then cease monitoring. A few days later, the federal investigators monitor the suspect for another five days and then stop. If seven days of GPS monitoring constitutes a search, whether a search has occurred depends on whether courts aggregate the days across the two investigations.¹⁴²

C. The Constitutional Reasonableness of Mosaic Searches

After courts define the standard for the mosaic theory and develop a theory of grouping, they must next articulate a framework for analyzing the reasonableness of mosaic searches. Recall that constitutional reasonableness requires a balancing of interests. Courts weigh the invasiveness of the government conduct against the extent to which it serves legitimate government interests, and they then determine how much regulation of that step is needed to ensure its use is constitutionally reasonable.¹⁴³ For some searches, courts require a warrant based on probable cause.¹⁴⁴ For other searches, they require just probable cause, or reasonable suspicion, or even no suspicion at all.¹⁴⁵ How should this framework apply to mosaic searches? Should mosaic searches require search warrants, and if so, how should such warrants be drafted? If warrants are not required, what level of cause must be established?

The question is difficult because the reasonableness of searches traditionally has been tied to the location of the place searched and the circumstances in which the search occurred. Searches of homes ordinarily require a warrant.¹⁴⁶ Searches of cars ordinarily require probable cause but

141. These issues did not come up in *Maynard/Jones* because the government did not seek admission of the cell-site monitoring, and it seems that the visual surveillance did not cover the location information revealed by the GPS device and used at trial.

142. Different investigations might represent different governments, different agencies of the same government, different parts of the same agency, or a mix of these options. They might know of each other, or they might not.

143. See *United States v. Place*, 462 U.S. 696, 703 (1983); *United States v. Bailey* (*In re Subpoena Duces Tecum*), 228 F.3d 341, 348-49 (4th Cir. 2000).

144. See *United States v. Karo*, 468 U.S. 705, 719 (1984).

145. Compare *California v. Carney*, 471 U.S. 386, 392-94 (1985), with *Terry v. Ohio*, 392 U.S. 1, 30 (1968).

146. See *Karo*, 468 U.S. at 719.

no warrant.¹⁴⁷ Limited frisks of persons for weapons require only reasonable suspicion that a suspect is armed and dangerous.¹⁴⁸ And most of these searches can be performed with less or even no suspicion in special circumstances, ranging from searches of probationers (no suspicion required)¹⁴⁹ to searches under exigent circumstances (general reasonableness required).¹⁵⁰

Applying these principles to mosaic searches raises novel issues because mosaic searches target a “place” that has never before been regulated under the Fourth Amendment. In *Maynard/Jones*, for example, GPS monitoring collected information about Jones’s public location. The justices agreed that the government conduct constituted a search, but they did not reach the reasonableness of the search because the question was not litigated below.¹⁵¹ If the justices had reached the question, the pro-mosaic justices would have had to decide a question of first impression: what is the reasonableness of a search of public space? No court has ever considered the question before *Jones* because public-location surveillance has not been considered a “search.”¹⁵²

Several different outcomes seem plausible. Some Fourth Amendment precedents present the warrant requirement as a default and suggest that a specific exception must be articulated for another standard to apply.¹⁵³ If courts follow those cases, they might conclude that mosaic searches require a warrant simply because there is no strong reason not to apply a warrant requirement.¹⁵⁴ Courts also might say that mosaic searches require a warrant because mosaic searches are quite invasive when considered cumulatively or that the benefit of ex ante judicial review makes a warrant requirement reasonable.¹⁵⁵

On the other hand, other precedents focus more on the Fourth Amendment’s requirement of reasonableness.¹⁵⁶ Courts could apply those precedents

147. See *Carney*, 471 U.S. at 392–94.

148. *Terry*, 392 U.S. at 27.

149. *Samson v. California*, 547 U.S. 843, 857 (2006).

150. *Kentucky v. King*, 131 S. Ct. 1849, 1858 (2011).

151. *United States v. Jones*, 132 S. Ct. 945, 954 (2012).

152. To be sure, in *United States v. Karo*, the Supreme Court did rule that use of a radio beeper to determine the location of property inside a home requires a warrant. 468 U.S. 705, 714 (1984). But the reason was that the beeper disclosed information about the inside of a home, which traditionally requires a warrant. See *id.* at 718–19.

153. E.g., *Katz v. United States*, 389 U.S. 347, 357 (1967) (“[S]earches conducted outside the judicial process, without prior approval by judge or magistrate, are *per se* unreasonable under the Fourth Amendment—subject only to a few specifically established and well-delineated exceptions.”).

154. E.g., *State v. Zahn*, 812 N.W.2d 490, 499 (S.D. 2012) (suggesting that a warrant is required for mosaic searches because no exception to the warrant requirement applies).

155. See, e.g., *id.* (“Because the unfettered use of surveillance technology could fundamentally alter the relationship between our government and its citizens, we require oversight by a neutral magistrate.”).

156. See, e.g., *Illinois v. McArthur*, 531 U.S. 326, 330 (2001) (noting that the “central requirement” of the Fourth Amendment “is one of reasonableness,” which has led the Supreme Court to “interpret[] the Amendment as establishing rules and presumptions designed to

to conclude that mosaic searches are less invasive than home searches and therefore do not require a warrant. For example, courts might analogize mosaic searches to car searches. Just as persons only have a reduced expectation of privacy in their cars in part because cars are exposed to public view, justifying less Fourth Amendment protection for cars than homes,¹⁵⁷ perhaps persons have only a reduced expectation of privacy in open spaces that are “searched” by the mosaic.

The reasonableness of mosaic searches becomes particularly complicated if courts conclude that multiple kinds of surveillance practices trigger the mosaic inquiry. Courts will need to consider if the reasonableness of a mosaic search is a “one-size-fits-all” question or if different kinds of mosaics implicate different reasonableness standards. For example, perhaps GPS mosaic searches are so invasive that they require a warrant, but cell-site mosaic searches—being less detailed and accurate than GPS mosaic searches—require only probable cause. Or perhaps mosaic searches operate on a graduated scale, requiring less suspicion when they first trigger the mosaic threshold but then requiring greater suspicion and a warrant as the surveillance continues.

Courts will next need to answer what kind of probable cause or reasonable suspicion is required. Probable cause and reasonable suspicion represent levels of probability. But what these standards mean depends on the context. The question is, *probability of what?* When the Fourth Amendment requires probable cause to arrest, for example, the relevant probable cause is probable cause to believe that a crime has been committed and that the suspect committed it.¹⁵⁸ When the Fourth Amendment requires search warrants, however, the probable cause requirement refers to probable cause to believe that evidence or contraband will be found inside the place to be searched.¹⁵⁹ The meaning of probable cause depends on the context, with different kinds of searches and seizures requiring different kinds of probable cause.

This prompts an intriguing question: if mosaic searches require probable cause, then what kind of probable cause do they require? Must investigators establish probable cause to believe that the location of the suspect is evidence of a crime? Must they establish probable cause to believe that the suspect monitored has committed a crime? Or perhaps some other standard applies?

A recent decision demonstrates the difficulty.¹⁶⁰ Investigators looking for a fugitive applied for a warrant to collect both GPS and cell-site location evidence in an effort to locate the fugitive and prosecute him. The govern-

control conduct of law enforcement officers that may significantly intrude upon privacy interests” that “[s]ometimes . . . require warrants” and other times do not (quoting *Texas v. Brown*, 460 U.S. 730, 739 (1983)) (internal quotation marks omitted)).

157. See, e.g., *California v. Carney*, 471 U.S. 386, 392–94 (1985).

158. *Warden v. Hayden*, 387 U.S. 294 (1967).

159. *Id.* at 307.

160. See *In re Application of the U.S. for an Order Authorizing Disclosure of Location Info. of a Specified Wireless Tel.*, No. 10-2188-SKG, 2011 WL 3423370 (D. Md. Aug. 3, 2011).

ment's application established probable cause to believe that the monitoring would help find the fugitive and that the fugitive was wanted for violations of federal law. The magistrate judge rejected the government's application because the government proved the wrong kind of probable cause. In the magistrate's opinion, the Fourth Amendment requires probable cause that the evidence sought by the warrant was itself evidence of a crime.¹⁶¹ The Fourth Amendment did not permit the issuance of a warrant because the fugitive's current location was not itself evidence of a crime.¹⁶²

If courts conclude that mosaic searches require a warrant, they also must answer how courts can satisfy the particularity requirement of the Warrant Clause. The Fourth Amendment states that warrants must "particularly describ[e] the place to be searched, and the persons or things to be seized."¹⁶³ But what is the specific "place" to be searched in a mosaic search? By their nature, mosaic searches aggregate across many places. The concept of mosaic searches draws on the fact that they bring together information from many places and instances to create a detailed picture of a suspect's life. The search does not occur in any one place. What is the "place" to be searched? The world? The court's jurisdiction? Or perhaps the collective places where the suspect happens to go?

The issue is particularly complex if the mosaic theory regulates beyond the collection of evidence to include its analysis and use.¹⁶⁴ Should the "place" where the search takes place include where the analysis and use take place or only where the collection occurs? Similar problems arise with the requirement of particularly describing the "thing" to be "seized." Mosaic searches do not seem to "seize" anything. Rather, they collect information about a person's whereabouts and life. And assuming *something* is seized over the course of a mosaic,¹⁶⁵ how can a warrant describe that thing to be seized with the specificity needed to satisfy the particularity requirement? The question is difficult because the purpose of the requirement is to ensure that searches remain narrow: searches must be limited to a single place and a hunt for specific evidence.¹⁶⁶ The theory of mosaic searches flips this understanding on its head. Mosaic investigations are deemed searches precisely because they are *not* limited. Given these difficulties, it is unclear how or whether courts can reconcile the mosaic search theory and the particularity requirement.¹⁶⁷

161. See *id.* at *27–30.

162. *Id.* at *30.

163. U.S. CONST. amend. IV.

164. See *supra* Section III.A.2.

165. Cf. *United States v. Freitas*, 800 F.2d 1451, 1455 (9th Cir. 1986) (noting that a warrant rule permitting officers to obtain a warrant to seize property authorizes the police to obtain a sneak-and-peek because entry into a space "seizes" information about what is inside it).

166. See U.S. CONST. amend. IV.

167. Courts have encountered somewhat related questions before, although the guidance in those precedents is only modestly helpful. In *United States v. Karo*, the Supreme Court suggested that when the police needed to obtain a warrant to use a radio beeper, the place to

D. Remedies for Mosaic Searches

The final set of questions concerns the scope of remedies for unconstitutional mosaic searches. Three questions must be answered: first, whether the exclusionary rule should apply to mosaic search violations; second, who has standing to challenge mosaic searches; and third, the proper scope of the fruit of the poisonous tree and inevitable discovery doctrines.

1. Does the Exclusionary Rule Apply?

The first significant question is whether mosaic search violations should trigger the exclusionary rule. Under the exclusionary rule, the government cannot use at trial evidence obtained in violation of the Fourth Amendment. The scope of the exclusionary rule is complex and currently in a state of considerable flux. But the scope of the exclusionary rule for mosaic violations would raise particularly difficult questions.

The first question is whether mosaic violations would be categorically exempt from the exclusionary rule under *Hudson v. Michigan*.¹⁶⁸ In *Hudson*, the Supreme Court held that the suppression remedy is not available for violations of the Fourth Amendment “knock-and-announce” rule.¹⁶⁹ The knock-and-announce rule generally requires agents executing warrants to first knock on the door and announce their presence, and then wait a “reasonable time” before entering the place to be searched.¹⁷⁰ *Hudson* concluded that suppression for knock-and-announce violations was inappropriate because the costs of the exclusionary rule in that setting outweighed its benefits. The murkiness of exactly what the “reasonable time” standard requires would trigger endless litigation,¹⁷¹ and it was likely that the combination of civil remedies and the training of professional officers would lead to substantial compliance with the rule even without a suppression remedy.¹⁷²

be searched was “the object into which the beeper is to be placed.” 468 U.S. 705, 718 (1984). This guidance does not answer how particularity applies in the case of the mosaic theory, however, as the mosaic theory applies to the collection of evidence over time rather than the installation of a device. See *United States v. Jones*, 132 S. Ct. 945, 957–58 (2012) (Alito, J., concurring in the judgment).

Case law on the particularity requirement for roving wiretaps provides another reference point that is of only limited value. Investigators can obtain roving wiretap orders when suspects frequently change phones; the orders allow the government to monitor phone calls over whatever telephone facilities the suspects use. Although lower courts have upheld the roving wiretap authority, e.g., *United States v. Petti*, 973 F.2d 1441, 1445 (9th Cir. 1992), roving wiretaps still state the place to be searched, e.g., *id.* (“Only telephone facilities actually used by an identified speaker may be subjected to surveillance . . .”). In other words, the place to be searched is the specific telephone facility where the suspect is placing a phone call. In the case of a mosaic, in contrast, it is axiomatic that the search cannot occur in a single place.

168. 547 U.S. 586 (2006).

169. *Hudson*, 547 U.S. at 599.

170. *Wilson v. Arkansas*, 514 U.S. 927, 931–34 (1995).

171. See *Hudson*, 547 U.S. at 594–95, 598.

172. See *id.* at 598–99.

If courts recognize mosaic searches, they will need to consider whether mosaic violations are exempt from the exclusionary rule under *Hudson*. On one hand, courts might plausibly analogize mosaic search violations to knock-and-announce violations. Both involve murky standards and would likely draw significant litigation. To the extent civil remedies and professionalism ensure that officers comply with the knock-and-announce rule, the same reasoning might suggest that officers can comply with the mosaic search rules (whatever they turn out to be). On the other hand, courts could distinguish mosaic searches on the ground that they are more directly related to the discovery of evidence. In knock-and-announce cases, the violation and discovery of evidence generally are unrelated. Failing to knock and announce does not change the evidence discovered.¹⁷³ In contrast, if investigators use tools that create a mosaic of a suspect, at least some parts of the mosaic are likely to lead to information that could be used in court if it reveals evidence of crime.

If courts reject *Hudson* as a basis for denying an exclusionary remedy for mosaic searches, the good-faith exception to the exclusionary rule may nonetheless substantially narrow its application. The Supreme Court's most recent cases on the good-faith exception indicate that the exclusionary rule does not apply unless an officer acted culpably.¹⁷⁴ Although the cases are not a model of clarity, they seem to indicate that the violation must be intentional, reckless, or grossly negligent to justify suppression.¹⁷⁵ Otherwise, the violation is one in "good faith" and no exclusionary rule applies.¹⁷⁶ Depending on how courts implement the mosaic theory, a plausible argument exists that the good-faith exception may apply to many types of mosaic searches. If courts cannot specify *ex ante* with clarity when police conduct aggregates sufficiently to constitute a search, officers may understandably cross the line without personal culpability. Unless the violation is a brazen one, the exclusionary rule might not apply.

Privacy statutes may also limit the scope of the exclusionary rule. Under *Illinois v. Krull*,¹⁷⁷ the exclusionary rule does not apply if officers reasonably rely on statutes that authorize their conduct. State laws regulating GPS surveillance may provide a basis for reasonable reliance.¹⁷⁸ To the extent the scope of the mosaic theory remains unclear, officers who follow statutes regulating GPS surveillance are likely to avoid suppression even if courts

173. See *id.* at 603 (Kennedy, J., concurring in part and concurring in the judgment).

174. See, e.g., *Davis v. United States*, 131 S. Ct. 2419, 2427–28 (2011).

175. See *id.* (citing *Herring v. United States*, 555 U.S. 135, 137 (2009)).

176. See *id.*

177. 480 U.S. 340, 355 (1987).

178. For example, Minnesota Statute sections 626A.35 through 626A.37 require the government to obtain a court order to install a mobile tracking device, and authorize surveillance for up to sixty days based on proof of "reason to believe that the information likely to be obtained by the installation and use is relevant to an ongoing criminal investigation." MINN. STAT. ANN. § 626A.37 (West 2009). This appears to be a lower standard than probable cause. See *State v. Fakler*, 503 N.W.2d 783, 786–87 (Minn. 1993) (analyzing the "reason to believe" standard in the Minnesota state surveillance statutes).

take a more restrictive view of the GPS surveillance than do the relevant statutes.¹⁷⁹

2. Standing to Challenge Mosaic Searches

If the exclusionary rule generally applies to mosaic search violations, courts will need to determine its scope. The first challenge is identifying who has standing to challenge a mosaic search. Fourth Amendment rights are personal, and individuals can invoke a remedy only if their own rights have been violated.¹⁸⁰ The Fourth Amendment standing inquiry arises as an application of the reasonable expectation of privacy test. Every defendant must establish that his or her own reasonable expectation of privacy was violated to merit a ruling suppressing the evidence.¹⁸¹

Standing raises difficult challenges for the mosaic theory because conduct that creates a mosaic may involve monitoring different people at different times to different degrees. Consider the facts of a recent district court case, *United States v. Luna-Santillanes*.¹⁸² Three conspirators ran a heroin trafficking enterprise and shared three cars. Different drivers drove the three different cars at different times. Investigators installed GPS devices on all three cars and used the GPS devices to track the movements of the three defendants.¹⁸³ The first car was monitored for two months; the second car was monitored for what the court called “a few” days; and the third car was monitored for only two days.¹⁸⁴

Assuming that the collective monitoring of the three cars constituted a search, who has standing to challenge it? Do all three defendants have standing because their location was monitored as part of a broader mosaic? Or must the standing inquiry look to each individual and consider whether the monitoring of that particular defendant was enough to constitute its own mosaic? Or perhaps the standing inquiry should operate on a car-by-car basis, limiting standing to primary drivers or passengers of particular cars?¹⁸⁵ If the exclusionary rule applies to mosaic searches, courts will need to develop answers to these questions.

179. In the short term, the good-faith exception to the exclusionary rule for reliance on binding appellate precedent might also play a role. See *Davis*, 131 S. Ct. at 2423–24 (extending the good-faith exception to reliance on binding appellate precedent). Application of *Davis* to mosaic searches is murky, however, as it remains unclear to what extent the discrete-steps approach factors in reliance on binding precedent. See *id.*

180. *Minnesota v. Carter*, 525 U.S. 83, 99 (1998) (Kennedy, J., concurring) (“Fourth Amendment rights are personal, and when a person objects to the search of a place and invokes the exclusionary rule, he or she must have the requisite connection to that place.”).

181. See *Rakas v. Illinois*, 439 U.S. 128 (1978).

182. No. 11-20492, 2012 WL 1019601, at *1 (E.D. Mich. Mar. 26, 2012).

183. *Luna-Santillanes*, 2012 WL 1019601, at *1–4.

184. *Id.* at *7 n.4.

185. Cf. *United States v. Hanna*, No. 11-20678-CR, 2012 WL 279435, at *4 (S.D. Fla. Jan. 30, 2012) (“For purposes of this analysis under *Jones*, one must have an expectation of privacy as to the particular vehicle tracked, either from an ownership or possessory interest.”).

3. Fruit of the Poisonous Tree and Inevitable Discovery

Assuming the exclusionary rule applies and defendants have standing, the next question is whether the unconstitutional conduct justifies suppression because it acts as both the but-for and proximate cause of the discovery of the relevant evidence. In the context of the exclusionary rule, these questions arise under the rubric of the “fruit of the poisonous tree” and “inevitable discovery” doctrines.¹⁸⁶ These doctrines raise puzzling questions for mosaic violations because it is difficult to identify the unconstitutional mosaic act. Is the aggregated mosaic a single unconstitutional act, or is the unconstitutional act only the surveillance that occurred after the monitoring became a search?

Consider whether the exclusionary rule applies to the entire mosaic or only some part of it. To simplify matters, let’s use the prior assumption that seven days of GPS monitoring crosses the line to become a search. If the police monitor a GPS device for ten days, must the entire ten days of monitoring be suppressed? Or should courts only suppress the last three days of monitoring data that occurred after the search line was crossed? Further, imagine the police learn on day two of the ongoing surveillance that the suspect committed a crime. Should the evidence from day two be suppressed because it was part of the mosaic triggered after seven days, even though the collection of that evidence was not a search when it occurred? Or is the evidence from day two an inevitable discovery because it would have been discovered if the monitoring had stopped before the amount of monitoring crossed the mosaic threshold?

A related issue arises when investigators use surveillance to locate targets at a particular moment rather than to develop a picture of their lives over time. Consider a recent case involving a GPS device attached to a car used to transport heroin.¹⁸⁷ Investigators used GPS tracking to find the car. After finding the car, officers conducted a pretextual traffic stop based on a traffic violation, asked for and obtained consent to search the car, and then retrieved two kilograms of heroin inside.¹⁸⁸ Assuming the GPS device was used long enough to cross the threshold of a search, should the heroin be suppressed as a fruit of the poisonous mosaic search? Or does the exclusionary rule not apply because the stop was the product of a short-term use of the GPS device rather than a broader mosaic? Again, these are difficult questions that courts will have to answer if they embrace a mosaic theory.

IV. THE CASE AGAINST THE MOSAIC THEORY

The five votes in favor of a mosaic approach in *United States v. Jones*¹⁸⁹ do not establish the theory as a matter of law. The majority opinion in *Jones*

186. See *supra* notes 51–53 and accompanying text.

187. *Luna-Santillanes*, 2012 WL 1019601, at *1–2.

188. See *id.*

189. 132 S. Ct. 945 (2012).

did not adopt the mosaic approach, and it only touched on the method in passing to express skepticism.¹⁹⁰ Sequential precedents remain binding on lower courts even if five justices seem prepared to take a new path. For now, the sequential approach remains the basic standard of Fourth Amendment doctrine. At the same time, the concurring opinions in *Jones* invite lower courts to consider embracing some form of the mosaic approach. Our attention therefore must turn to the normative question: Should courts adopt the mosaic theory? Is the mosaic approach a promising new method of Fourth Amendment interpretation, or is it a mistake that should be avoided?

This Part argues that courts should reject the mosaic theory. The better course is to retain the traditional sequential approach to Fourth Amendment analysis. The mosaic theory aims at a reasonable goal. Changing technology can outpace the assumptions of existing precedents, and courts may need to tweak prior doctrine to restore the balance of privacy protection from an earlier age. I have called this process “equilibrium-adjustment,”¹⁹¹ and it is a longstanding method of interpreting the Fourth Amendment. But the mosaic theory aims to achieve this goal in a very peculiar way.

The mosaic theory amounts to an awkward halfway measure. Under the sequential approach, courts traditionally have two options when deciding how to regulate police conduct. They can decide that particular conduct is *never* a Fourth Amendment search but that legislatures can regulate the conduct by enacting statutory protections, or they can say that the conduct is *always* a Fourth Amendment search. The mosaic theory offers a vague middle ground as a third option. The theory allows courts to say that techniques are *sometimes* a search. They are not searches when grouped in some ways (when no mosaic exists) but become searches when grouped in other ways (when the mosaic line is crossed).

Identifying the principles that should govern this middle ground is extremely difficult, however, such that the challenges of the method outweigh its possible benefits. As Part III explained, implementing the mosaic theory raises a large number of novel and complex questions that courts would need to answer. It is hard to see how courts can answer all these questions coherently. Even proponents of the mosaic approach appear not to have answers for how it should apply.¹⁹² Rather than jump headfirst into this morass, the wiser course is to retain the two options presented under the sequential approach.

This does not mean that courts must allow technology to erode Fourth Amendment privacy. If courts must expand Fourth Amendment privacy protections in response to new technologies, they can conclude that the disputed conduct is always a search under a sequential analysis. The model for this approach is the most famous Fourth Amendment decision: *Katz v. United*

190. See *Jones*, 132 S. Ct. at 954 (referring to the approach articulated in Justice Alito’s opinion as “thorny,” “vexing,” and a “novelty,” and asking, “What of a 2-day monitoring of a suspected purveyor of stolen electronics? Or of a 6-month monitoring of a suspected terrorist?”).

191. See Kerr, *supra* note 16.

192. See *infra* notes 204–208 and accompanying text.

States.¹⁹³ Katz shows that rejecting the mosaic theory does not mean rejecting broad Fourth Amendment protection. It only means rejecting the awkward halfway measure of the mosaic theory.

A. The Mosaic Theory as Equilibrium-Adjustment

In a recent article,¹⁹⁴ I argued that much of modern Fourth Amendment doctrine reflects the principle of equilibrium-adjustment. When technology and social practice change in ways that substantially threaten the government's power to solve crimes, courts often respond by loosening Fourth Amendment rules to restore the prior level of investigatory power. On the other hand, when technology and social practice considerably expand government power, courts respond by strengthening Fourth Amendment rules to attempt to restore the prior level of constitutional protection. Judges interpret the Fourth Amendment in response to major technological changes much like a driver trying to maintain speed on hilly terrain: they add gas when climbing uphill but lay off the pedal on the downward slopes.¹⁹⁵

The mosaic theory of the Fourth Amendment fits nicely into this framework. Computerization enables extremely fast repetition of surveillance practices. If a computer can do something, it can do that thing many times in a split second. Computers also have a previously unimaginable capacity to aggregate and analyze whatever information investigators collect. The mosaic theory attempts to restore the balance of power by disabling the government's ability to rely on what computerization enables. As Justice Alito noted in *Jones*, surveillance in "the pre-computer age" was necessarily limited, while computers changed massive-scale monitoring from something "impractical" to something "relatively easy and cheap."¹⁹⁶ Such new powers "may 'alter the relationship between citizen and government,'" ¹⁹⁷ Justice Sotomayor worried, resulting in "a tool so amenable to misuse"¹⁹⁸ that Fourth Amendment doctrine needed to respond.

The mosaic theory aims to restore the balance of police power by labeling the government's enhanced powers as searches. If investigators use new tools in modest ways consistent with earlier government capacities, their use remains outside the scope of Fourth Amendment protection. But if the government fully exploits the new powers the new tools provide, the scope of surveillance upsets the earlier balance and the mosaic theory subjects the government's conduct to Fourth Amendment oversight.

193. 389 U.S. 347 (1967).

194. See Kerr, *supra* note 16.

195. See *id.* at 487–90 (explaining the process of equilibrium-adjustment).

196. See *United States v. Jones*, 132 S. Ct. 945, 963–64 (2012) (Alito, J., concurring in the judgment).

197. *Id.* at 956 (Sotomayor, J., concurring) (quoting *United States v. Cuevas-Perez*, 640 F.3d 272, 285 (7th Cir. 2011) (Flaum, J., concurring), *vacated*, 132 S. Ct. 1534 (2012) (mem.)).

198. *Id.* (quoting *United States v. Di Re*, 332 U.S. 581, 595 (1948)) (internal quotation marks omitted).

B. *The Case Against the Mosaic Theory*

The critical question is whether the mosaic theory offers a desirable approach to equilibrium-adjustment. 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.

1. The Mosaic Theory Would Be Very Difficult to Administer

The first difficulty with the mosaic theory is the most obvious: its implementation raises so many difficult questions that it will prove exceedingly hard to administer effectively. Because the mosaic theory departs dramatically from existing doctrine, implementing it would require the creation of a new set of Fourth Amendment rules—in effect, a mosaic parallel to the sequential precedents that exist today. The problem is not only the number of questions but also their difficulty. Many of the questions raised in Part III of this Article are genuine puzzles that Fourth Amendment text, principles, and history cannot readily answer. Judges should be reluctant to open the legal equivalent of Pandora's Box.

Murky standards are not unknown in Fourth Amendment law, of course. But the murkiness of the mosaic theory is unprecedented. I find it particularly telling that not even the proponents of the mosaic theory have proposed answers for how the theory should apply. For example, in one recent article, a group of scholars who endorsed the mosaic approach dismissed the conceptual difficulties of its implementation on the ground that answering such puzzles “is why we have judges.”¹⁹⁹ A pro-mosaic amicus brief in *Jones* signed by several prominent legal academics was similarly nonresponsive.²⁰⁰ The brief brushed off the difficulties with implementing the mosaic theory by stating that judges encounter vague standards elsewhere in Fourth Amendment law and they can implement the mosaic theory by “consider[ing] the same criteria applied to other surveillance situations.”²⁰¹

I appreciate such confidence in judicial abilities. But surely there is a stark difference between applying vague standards and implementing a the-

199. See Smith et al., *supra* note 15, at 201.

200. See Brief of *Amici Curiae*, Yale Law School Information Society Project Scholars and Other Experts in the Law of Privacy and Technology in Support of the Respondent at 25–27, *Jones*, 132 S. Ct. 945 (No. 10-1259), 2011 WL 4614429. The scholars who signed onto this brief included Daniel Solove, Paul Ohm, Danielle Citron, Christopher Slobogin, Susan Freiwald, Renee Hutchins, Chris Hoofnagle, and Stephen Henderson. *Id.* at 1–3.

201. *Id.* at 27.

ory so mysterious that Fourth Amendment experts decline to express an opinion on how to apply it. Judges are smart people, but they are not like Moses bringing the tablets down from Mount Sinai. If the questions raised by the mosaic theory can be answered, proponents of the theory should answer them. Expressions of confidence that answers can be found do not substitute for the answers themselves.²⁰²

The challenge of answering the questions raised by the mosaic theory has particular force because the theory attempts to regulate use of changing technologies. Law enforcement implementation of new technologies can occur very quickly, while judicial resolution of difficult constitutional questions typically occurs at a more snail-like pace. As a result, the constantly evolving nature of surveillance practices can lead new questions to arise faster than courts might settle them. Old practices would likely be obsolete by the time the courts resolved how to address them, and the newest surveillance practices would arrive and their legality would be unknown. Like Lucy and Ethel trying to package candy on the ever-faster conveyor belt,²⁰³ the mosaic theory could place judges in the uncomfortable position of trying to settle a wide range of novel questions for technologies that are changing faster than the courts can resolve how to regulate them.

Consider the changes in location-identifying technologies in the last three decades. Thirty years ago, the latest in police location-tracking technologies was the primitive radio beeper seen in *Knotts*. But radio beepers are obsolete. Today the police have new tools at their disposal that were unknown in the *Knotts* era, ranging from GPS devices to cell-site records to license plate cameras. The rapid pace of technological change creates major difficulties for courts trying to apply the mosaic theory: if the technological facts of the mosaic change quickly over time, any effort to answer the many difficult questions raised by the mosaic theory will become quickly outdated. Courts eventually may devise answers to the many questions discussed in Part III. But by the time they do, the technology is likely to be obsolete.

202. The closest any scholar has come to answering the questions raised by the mosaic theory is Christopher Slobogin, who recently proposed a model statute to implement the mosaic theory. See Christopher Slobogin, *Making the Most of Jones v. United States in a Surveillance Society: A Statutory Implementation of Mosaic Theory*, 8 DUKE J. CONST. L. & PUB. POL'Y (forthcoming 2013), available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2098002. Professor Slobogin proposes a complex framework distinguishing among "target public searches," "targeted data search of data held by an institutional third party," and "general public and data searches." He would require different standards to conduct different kinds of surveillance for different times, such as twenty minutes or forty-eight hours. See *id.* at 17–22. Importantly, even Professor Slobogin declines to say how the mosaic theory applies. His proposal is statutory rather than constitutional. Further, Professor Slobogin's statutory proposal is similar to arguments he advanced in a recent book on the Fourth Amendment published well before *Jones*. See CHRISTOPHER SLOBOGIN, *PRIVACY AT RISK: THE NEW GOVERNMENT SURVEILLANCE AND THE FOURTH AMENDMENT* (2007)). I reviewed Professor Slobogin's book in 2009, and my critique of his approach then largely responds to his current proposal. See Orin S. Kerr, Review, *Do We Need a New Fourth Amendment?*, 107 MICH. L. REV. 951 (2009).

203. See *I Love Lucy: Job Switching* (CBS television broadcast Sept. 15, 1952).

2. Probabilistic Approaches to the "Reasonable Expectation of Privacy" Test Are Ill Suited to Regulate Technological Surveillance

The second problem with the mosaic theory is that most formulations are based on a probabilistic approach to the reasonable expectation of privacy test that proves ill suited to regulate technological surveillance practices. Supreme Court decisions have used several different inquiries to determine what makes an expectation of privacy constitutionally reasonable.²⁰⁴ In some cases, the Court has looked to what a reasonable person would perceive as likely;²⁰⁵ in other cases, the Court has looked to whether the particular kind of information obtained is worthy of protection;²⁰⁶ in some cases, the Court has looked to whether the government violated some legal norm such as a property right in obtaining the information;²⁰⁷ and in other cases, the Court has simply considered whether the conduct should be regulated by the Fourth Amendment as a matter of policy.²⁰⁸ Use of these multiple inquiries (what I have called "models") of Fourth Amendment protection allows the Court to adopt different approaches in different contexts, ideally selecting the model that best identifies the need for regulation in that particular setting.²⁰⁹

For the most part, formulations of the mosaic theory rest on the first of these approaches—what a reasonable person would see as likely. I have called this the probabilistic approach to Fourth Amendment protection,²¹⁰ as it rests on a notion of the probability of privacy protection. The more likely it is that a person will maintain their privacy, the more likely it is that government conduct defeating that expectation counts as a search. Under this model, the Fourth Amendment guards against surprises. The paradigmatic example is *Bond v. United States*,²¹¹ which involved government agents physically manipulating a bus passenger's duffel bag to identify a wrapped brick of drugs inside it. Manipulating the bag violated a reasonable expectation of privacy because a bus passenger expects other passengers to handle his bag but not to "feel the bag in an exploratory manner."²¹² Both Judge Ginsburg and Justice Alito authored mosaic opinions that rely on such probabilistic reasoning.²¹³ Judge Ginsburg deemed long-term GPS monitoring a search because no stranger could conduct the same level of monitoring as a GPS device. Justice Alito reached the same result on the grounds that a rea-

204. See Kerr, *supra* note 90.

205. See *id.* at 508–12.

206. See *id.* at 512–15.

207. See *id.* at 516–19.

208. See *id.* at 519–22.

209. See *id.* at 543–48.

210. See *id.* at 508–12.

211. 529 U.S. 334 (2000).

212. *Bond*, 529 U.S. at 339.

213. See *supra* Section II.B.

sonable person would not expect the police to obtain so much information.²¹⁴

The probabilistic approach is a poor choice to regulate technological surveillance, however. The problem is a practical one. Most individuals lack a reliable way to gauge the likelihood of technological surveillance methods. The probabilistic expectation of privacy applied in *Bond* relied on widespread and repeated personal experience. Bus passengers learn the social practices of bus travel by observing it firsthand. In contrast, estimating the frequency of technological surveillance practices is essentially impossible for most people (including most judges). Surveillance practices tend to be hidden, and few understand the relevant technologies. Some people will guess that privacy invasions are common. Others will guess that they are rare. But exceedingly few will know the truth, which makes probabilistic beliefs a poor basis for Fourth Amendment protection.

Consider the so-called “CSI effect,”²¹⁵ by which jurors in routine criminal cases expect prosecutors to introduce evidence collected using high-tech investigatory tools like those featured on popular television dramas such as *Law & Order* and *CSI*. The CSI effect suggests that members of the public derive their expectations of police practices in large part from entertaining but largely fictional television shows. Resting Fourth Amendment doctrine on such malleable expectations seems a curious choice. A hit show featuring hardworking officers with high-tech tools could cut back Fourth Amendment protection by suggesting that very invasive investigations are commonplace. On the other hand, a new show featuring lazy or incompetent officers might expand Fourth Amendment protection by making particularly thorough investigations exceed societal expectations. It is hard to see why such poorly informed beliefs should shape Fourth Amendment protections.

Nor does Supreme Court doctrine require such a result. To the contrary, the Supreme Court has generally avoided applying the probabilistic model to government surveillance practices.²¹⁶ The Court has relied instead on other models that provide more stable ways to regulate government surveillance practices.²¹⁷ Courts should follow that lead, continuing to focus on the models of the reasonable expectation of privacy test that do not rely on probabilistic reasoning.

214. See *supra* Section II.C.

215. See Simon A. Cole & Rachel Dioso-Villa, *Investigating the ‘CSI Effect’ Effect: Media and Litigation Crisis in Criminal Law*, 61 STAN. L. REV. 1335, 1336–37 (2009).

216. See *United States v. Sparks*, 750 F. Supp. 2d 384, 392 (D. Mass. 2010) (“Rather than using a probabilistic approach to determine reasonable expectations of privacy, in the context of governmental use of new technologies, the Supreme Court repeatedly has focused on whether the nature of the information revealed is private and thus worthy of constitutional protection.”).

217. See *id.*

3. The Mosaic Theory Could Interfere with More Effective Statutory Protections

A third difficulty with the mosaic theory is that it may interfere with the development of statutory privacy laws. As I have explained in another article²¹⁸—and as Justice Alito suggested in his concurring opinion in *Jones*²¹⁹—Congress has significant institutional advantages over the courts in trying to regulate privacy in new technologies. Congress can act quickly, hold hearings, and consider expert opinion.²²⁰ Congress can draw arbitrary lines that don't fit easily within constitutional doctrine.²²¹ And if Congress errs or facts change, Congress can amend its prior handiwork relatively easily.²²² Congress can also regulate using sunset provisions that force the legislature to revisit the question in light of intervening experience.²²³ For these reasons, legislative privacy laws have considerable institutional advantages over the products of the comparatively slow and less-informed judicial process.

The mosaic approach could interfere with statutory solutions in two ways. First, the theory might discourage legislative action by fostering a sense that the courts have occupied the field.²²⁴ When courts hear a controversial privacy case but rule that the Fourth Amendment does not apply, the judicial “no” identifies a problem for the legislature to address. The absence of judicial regulation invites legislative action. Prominent examples include the Right to Financial Privacy Act of 1978,²²⁵ passed in response to *United States v. Miller*;²²⁶ the Pen Register Statute,²²⁷ passed in response to *Smith v. Maryland*;²²⁸ and the Privacy Protection Act of 1980,²²⁹ passed in response to *Zurcher v. Stanford Daily*.²³⁰ In all three instances, Congress responded to a Fourth Amendment ruling allowing a controversial investigatory practice

218. See Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 855–57 (2004).

219. See *Jones*, 132 S. Ct. 945, 964 (2012) (Alito, J., concurring in the judgment) (citing Kerr, *supra* note 90, at 805–06).

220. Kerr, *supra* note 90, at 870, 881–82.

221. See *id.* at 871–72.

222. See *id.*

223. See *id.* at 873.

224. Cf. *id.* at 855–57.

225. Pub. L. No. 95-630, tit. XI, 92 Stat. 3641, 3697–710 (codified at 12 U.S.C. §§ 3401–3422 (2006)).

226. 425 U.S. 435 (1976).

227. Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, sec. 301(a), 100 Stat. 1848, 1868–72 (codified as amended at 18 U.S.C. §§ 3121–3127 (2006 & Supp. IV 2010)).

228. 442 U.S. 735 (1979).

229. Pub. L. No. 96-440, 94 Stat. 1879 (codified as amended at 42 U.S.C. §§ 2000aa, 2000aa-5 to 2000aa-7, 2000aa-11 (2006)).

230. 436 U.S. 547 (1978).

by creating statutory protections.²³¹ The possibility of mosaic protection complicates the legislative picture because mosaic protections can overlap with possible statutory solutions and therefore render the case for statutory protection much less apparent.²³²

The two concurring opinions in *Jones* can be read as hinting at another possible interaction between the mosaic theory and statutory protections: perhaps the mosaic theory operates only where no statutory protection exists, such that enactment of statutory protections disables the mosaic theory.²³³ If so, the mosaic theory could encourage statutory protections rather than discourage them. But this possibility raises its own complex set of puzzles. For example, how many statutory protections suffice? At the time of *Jones*, a few state legislatures had already enacted GPS privacy

231. See, e.g., H.R. REP. NO. 95-1383, at 34 (1978), reprinted in 1978 U.S.C.C.A.N. 9273, 9306 (discussing bills to create statutory right to privacy in financial records in response to *United States v. Miller*, 425 U.S. 435).

232. This is just a prediction, of course, and the novelty of the mosaic approach makes it difficult to prove. One very modest piece of evidence might be the congressional action on location privacy before and after *Jones*. In the months leading up to the *Jones* decision, several prominent bills were introduced in Congress to regulate GPS surveillance. In June 2011, Senators Franken and Blumenthal introduced the Location Privacy Protection Act of 2011, S. 1223, 112th Cong. (2011), and Senator Wyden introduced the Geolocal Privacy and Surveillance Act, S. 1212, 112th Cong. (2011). In the months following *Jones*, however, those bills appear to be stalled, and no other bills have been introduced to date. Of course, one cannot draw much in the way of conclusions from such sparse evidence.

233. It is important to avoid reading too much into the penumbras of Supreme Court opinions. Such overreading can purport to find signals that no justice intended. With that said, Justice Alito introduces his mosaic solution in *Jones* by explaining that it is “[t]he best that we can do” in light of the fact that “to date . . . Congress and most States have not enacted statutes regulating the use of GPS tracking technology for law enforcement purposes.” *United States v. Jones*, 132 S. Ct. 945, 964 (2012) (Alito, J., concurring in the judgment). This statement could be interpreted in two ways. On one hand, perhaps it merely means that Justice Alito had to apply the Fourth Amendment because no statutes exist that could allow the Court to decide the legality of the government’s conduct without reaching the constitutional question. Under this interpretation, the “best that we can do” language merely reflects the principle of constitutional avoidance.

On the other hand, perhaps the “best that we can do” language means that the existence of privacy statutes disables the mosaic approach, or at least the possibility of an exclusionary remedy. Cf. *Illinois v. Krull*, 480 U.S. 340, 342, 349–50 (1987) (holding that the exclusionary rule does not apply when an officer reasonably relies on a statute authorizing investigatory conduct later ruled in violation of the Fourth Amendment). This latter interpretation is bolstered somewhat by the fact that even the widespread adoption of GPS statutes likely would not provide a basis for constitutional avoidance in *Jones*, at least outside the context of *Krull*’s good-faith exception. The federal agents in *Jones* would not be bound by a state GPS surveillance statute under the Supremacy Clause, and even a federal privacy statute could only resolve the *Jones* case to the extent it included a statutory suppression remedy.

Justice Sotomayor makes a somewhat similar suggestion in her statement that in applying the Fourth Amendment, she would “consider the appropriateness of entrusting to the Executive, in the absence of any oversight from a coordinate branch, a tool so amenable to misuse.” *Jones*, 132 S. Ct. at 956 (Sotomayor, J., concurring). This seems to suggest that oversight from a coordinate branch such as Congress might lead her to reach a different interpretation of the Fourth Amendment.

laws.²³⁴ A few state supreme courts had regulated GPS monitoring under state constitutions.²³⁵ More states and the federal government were likely to enact such protections in the future. If protections outside the Fourth Amendment end the need for Fourth Amendment protection, how many statutes and state constitutional decisions must be enacted before they are sufficient?

A related puzzle is how much protection such statutes must provide. If any statutory protection disables the mosaic, then legislatures can enact the most modest and toothless protection and that will suffice. The mosaic threat would be entirely procedural: legislatures would only need to check the box of establishing statutory protection to avoid a judicially enforced mosaic. On the other hand, if courts have to assess whether the statutes are sufficiently protective to address the kind of concerns that the mosaic theory addresses, then achieving that standard will be extremely difficult. For reasons I have explained in depth elsewhere, facial review of privacy statutes to determine if they are sufficiently protective to satisfy a general Fourth Amendment standard would trigger its own rather daunting interpretive challenges.²³⁶

C. The Mosaic Theory as a Halfway Measure and the Katz Example

Rejecting the mosaic theory does not mean that judges must sit idly by as advancing technology diminishes the role of the Fourth Amendment. Under the sequential approach, judges can engage in equilibrium-adjustment within the context of a binary choice. Judges can rule that government conduct is not a search and thereby leave it to statutory regulation, or they can decide it is a search and subject it to constitutional regulation. Rejecting the mosaic theory allows this process to continue. It simply leaves out the mosaic theory's effort to introduce a middle-ground third option that amounts to an awkward halfway measure.

The mosaic theory provides a halfway measure because it leaves sequential precedents partially in place. It leaves practices unregulated in some unspecified short-term contexts, and it then flips the switch and calls the government action a search when grouped together in some broader or longer-term contexts. Consider the use of GPS devices in *Maynard/Jones*. In *United States v. Knotts*, the Court had held that use of a location device to monitor the location of a car on public thoroughfares was never a search.²³⁷ In his mosaic concurrence in *Jones*, Justice Alito reaffirmed the *Knotts* precedent but limited it to "relatively short-term monitoring of a person's

234. See, e.g., FLA. STAT. § 934.06 (2011); MINN. STAT. ANN. § 626A.37 (West 2009).

235. See, e.g., *State v. Jackson*, 76 P.3d 217, 263–64 (Wash. 2003).

236. See Orin S. Kerr, *Congress, the Courts, and New Technologies: A Response To Professor Solove*, 74 *FORDHAM L. REV.* 779, 787–90 (2005).

237. 460 U.S. 276, 281–82 (1983).

movements on public streets.”²³⁸ Under this approach, *Knotts* was still good law—at least up to a point. Justice Alito’s mosaic opinion offered an attempted middle ground between retaining *Knotts* in its entirety or simply overturning it.

Although renouncing the mosaic theory would eliminate this middle ground, it would allow judges to continue to engage in equilibrium-adjustment by expanding what constitutes a search. The proper model is *Katz v. United States*,²³⁹ perhaps the most famous of all Fourth Amendment decisions. *Katz* expanded the scope of what constitutes a search by replacing the constitutionally protected area formulation with something broader. Under *Katz*, bugging and wiretapping that had been beyond Fourth Amendment protection were brought inside that protection to account for the new world of telephone communications. Notably, the *Katz* Court did not say that short-term bugging was permitted but that long-term bugging became a search at some unspecified point. Instead, the Court followed the traditional sequential approach by holding that *all* bugging of a phone while it was in a person’s private use triggered the Fourth Amendment.²⁴⁰

Application of the same method to the use of relatively new surveillance techniques such as GPS surveillance suggests that the Court should choose between two basic options. If technology and social practices remain sufficiently stable and the *Knotts/Karo* line properly balances law enforcement power and privacy rights, then courts should adhere to those cases. On the other hand, if changing technology and social practice dramatically expands government power under *Knotts/Karo*, courts can engage in equilibrium-adjustment and overturn *Knotts*. Courts should follow the *Katz* example and engage in equilibrium-adjustment within the confines of the sequential approach.

CONCLUSION

The concurring opinions in *Jones* invite lower courts to experiment with a new approach to the Fourth Amendment search doctrine. The approach is well intentioned. It aims to restore the balance of Fourth Amendment protection by disabling the new powers created by computerization of surveillance tools. But despite these good intentions, the mosaic theory represents a Pandora’s Box that courts should leave closed. The theory raises so many novel and difficult questions that courts would struggle to provide reasonably coherent answers. By the time courts worked through answers for any one technology, the technology would likely be long obsolete. Mosaic protection also could come at a cost of lost statutory protections, and implementing it would require courts to assess probabilities of surveillance that judges are poorly equipped to evaluate. The concurring

238. *United States v. Jones*, 132 S. Ct. 945, 964 (2012) (Alito, J., concurring in the judgment).

239. 389 U.S. 347 (1967).

240. *Katz*, 389 U.S. at 353, 359.

opinions in *Jones* represent an invitation that future courts should decline. Instead of adopting a new mosaic theory, courts should consider the need to engage in equilibrium-adjustment within the confines of the traditional sequential approach.

Article

When Database Queries Are Fourth Amendment Searches

Emily Berman[†]

INTRODUCTION

As anyone familiar with *Law & Order* knows, the Fourth Amendment demands that—before conducting a search or seizure—the government must secure a warrant. To be valid, the warrant must (1) be approved by a neutral decision-maker; (2) be based on a showing of probable cause; and (3) describe with particularity the places to be searched or the things to be seized.¹

Outside the world of police procedurals, however, the legal framework regulating the government’s investigative powers permits the collection of a great deal of information without abiding by prior approval, individualized cause,² or particularity requirements. Specifically, investigators need not meet traditional warrant requirements in at least two types of situations—warrant requirement exceptions and what I call “Fourth Amendment exemptions.”³ When an exception to the warrant requirement applies, the government satisfies Fourth Amendment demands merely by demonstrating that its actions are

[†] Assistant Professor of Law, University of Houston Law Center. Thanks go to Seth Chandler, Dave Fagundes, Barry Friedman, Aziz Huq, David Kwok, James Nelson, D. Theodore Rave, Jessica Roberts, Joe Sanders, and Greg Vetter, as well as participants in the 2016 Texas Legal Scholars workshop, the 2017 AALS National Security Law Section’s New Voices Panel, and the 2017 Michigan Young Scholars Conference, particularly Peter Margulies, Dakota Rudesill, and Margo Schlanger. All errors are the author’s. Copyright © 2017 by Emily Berman.

1. FED. R. CRIM. P. 41.

2. An “individualized suspicion” requirement demands that the government show cause—usually probable cause or reasonable suspicion—to believe that a search of a *particular* individual is justified. *United States v. Chandler*, 520 U.S. 305, 305–06 (1997).

3. *See infra* Part II.A.1.

reasonable.⁴ In Fourth Amendment exemptions, the government's collection activity does not violate a reasonable expectation of privacy and therefore the Fourth Amendment does not regulate the collection at all.⁵ Such investigative activity is considered neither a search nor a seizure, and is thus exempt from constitutional limitations. Together, warrant requirement exceptions and Fourth Amendment exemptions permit the government to lawfully scoop up an enormous volume of information about Americans, often without any reason to suspect any particular American of wrongdoing and with no demonstrated connection to crime or specific intelligence needs.

Moreover, there are no constitutional restrictions at all on how the government uses this vast expanse of data. So long as its collection is lawful, the Fourth Amendment has nothing to say about how information is employed.⁶ Rather, current constitutional doctrine allows the government to combine, compile, and analyze any information in its possession—even as the volume of this information becomes ever larger and analytical tools ever more powerful.

Courts and commentators recognize that the government's broad collection authority raises significant privacy concerns. The conventional response is to suggest expanding the scope of collection regulation, either by narrowing warrant requirement exceptions⁷ or broadening the definition of what qualifies as a search or seizure.⁸ Thus existing doctrine and extant reform

4. See, e.g., *Illinois v. Wardlow*, 528 U.S. 119, 126–27 (2000) (discussing the court's analysis of reasonable suspicion).

5. *Katz v. United States*, 389 U.S. 347 (1967). The reasonable-expectation-of-privacy inquiry asks first whether the government has violated an expectation of privacy, and second, whether society is prepared to accept that expectation as reasonable. *Id.* at 360 (Harlan, J., concurring); see also *infra* notes 77–80 and accompanying text.

6. See *infra* Part II.B.

7. E.g., BARRY FRIEDMAN, *UNWARRANTED: POLICING WITHOUT PERMISSION* (2017) (discussing policing reform in the United States).

8. The most common suggestion is to eliminate or constrain the third-party doctrine, which exempts from Fourth Amendment protections any information voluntarily conveyed to a third party. See, e.g., Erin Murphy, *The Case Against the Case for Third-Party Doctrine: A Response to Epstein and Kerr*, 24 *BERKELEY TECH. L.J.* 1239, 1252–53 (2009) (arguing that the third-party doctrine's application should vary based on the voluntariness with which the records were shared); Michael W. Price, *Rethinking Privacy: Fourth Amendment "Papers" and the Third-Party Doctrine*, 8 *J. NAT'L SEC. L. & POL'Y* 247, 249–50 (2015) (arguing that the government should be required to obtain a warrant prior to seizing some third-party data); Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 *S. CAL. L. REV.* 1083, 1157 (2002) [hereinafter Solove, *Digital Dossiers*] (arguing that the

proposals both accept as given that the Fourth Amendment's scope is limited to regulation of information collection. The privacy impact of large amounts of data, however, does not come solely from the sweeping nature of the government's *collection* authority. The government's postcollection *use* of information can—and often does—implicate privacy interests just as strongly.

This Article focuses on one form of information use with particularly troubling effects on privacy: database queries that implicate the aggregation problem.⁹ The aggregation problem, a label coined by Professor Daniel Solove, refers to the fact that the government can collect enough data—both in the sense of volume and of variety—that its aggregation and analysis can actually change the nature of the information, providing revelations that could not have been gleaned from the isolated bits of information alone.¹⁰ At a certain point, the whole equals more than the sum of its parts. Yet because such aggregation necessarily takes place only after the information is collected, the extraction of such revelations is not subject to any constitutional restrictions. I contend that when database queries about particular U.S. persons have the capacity to aggregate data such that it will reveal information that, in the absence of aggregation, the government could only access by conducting a search or seizure, the extraction of that information should be subject to constitutionally based limits.¹¹ In other words, when

third-party doctrine should apply only to “systems of records”); *see also* Klayman v. Obama, 957 F. Supp. 2d 1, 31 (D.D.C. 2013), *vacated and remanded*, 800 F.3d 559 (D.C. Cir. 2015) (arguing that the third-party doctrine does not apply to bulk collection of telephony metadata). *But see* Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561 (2009) (defending the third-party doctrine).

9. Solove, *Digital Dossiers*, *supra* note 8, at 1154.

10. *Id.*; Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477, 514 (2006) [hereinafter Solove, *A Taxonomy of Privacy*] (“Aggregation creates . . . a ‘digital person,’ a portrait composed of information fragments combined together.”); *see also* Joseph S. Fulda, *Data Mining and Privacy*, 11 ALB. L.J. SCI. & TECH. 105, 110 (2000) (noting that “two (conventional) data about an individual, each innocuous in itself” can together “produce new (conventional) knowledge about the individual”).

11. Database queries about particular U.S. persons are distinct from what is commonly labeled data mining. *See infra* notes 157–58 and accompanying text. This Article’s analysis is limited to U.S. person queries and leaves discussion of Fourth Amendment limits on data mining to future work. Indeed, there is already a vibrant and quickly growing literature regarding the constitutional implications of data mining. *E.g.*, Jane Bambauer, *Hassle*, 113 MICH. L. REV. 461 (2015) (discussing trends in policing technique); Andrew Guthrie Ferguson, *Big Data and Predictive Reasonable Suspicion*, 163 U. PA. L.

a database query returns information that the government could otherwise collect only through a Fourth Amendment-regulated means, the Fourth Amendment should regulate that query. If the government accesses an American's electronic communications, for example, the same expectation of privacy is violated—the expectation that the government does not have access to our private communications in the absence of a court order¹²—regardless of whether the government collected those communications directly, pursuant to a warrant, or accessed them by querying a database in which communications collected incidentally to the targeting of a non-American are stored.¹³ Note that the Constitution is triggered here by the nature of the information *exposed* by the query, not the nature of the information that makes up the underlying database(s).¹⁴

The Fourth Amendment should regulate information *use* as well as its *collection*, I argue, because no modification to the collection rules will address threats to privacy that come solely from information use.¹⁵ The digital age has rendered collection-focused efforts alone an insufficient means of preserving individual privacy, particularly in light of the fact that the government (1) is able to extract more information from the same data

REV. 327, 329–30 (2015) (discussing current trends toward “big data” and away from “small data”); Andrew Guthrie Ferguson, *Predictive Policing and Reasonable Suspicion*, 62 EMORY L.J. 259, 265 (2012) (analyzing possible effect of data analysis on policing); Elizabeth E. Joh, *Policing by Numbers: Big Data and the Fourth Amendment*, 89 WASH. L. REV. 35 (2014); Erin Murphy, *Databases, Doctrine & Constitutional Criminal Procedure*, 37 FORDHAM URB. L.J. 803, 812 (2010) (discussing the impact of databases on law enforcement).

12. United States v. U.S. Dist. Court (*Keith*), 407 U.S. 297 (1972) (so holding in the intelligence context); *Berger v. New York*, 388 U.S. 41 (1967) (so holding in the criminal context).

13. The reasonable-expectation-of-privacy test itself is generally recognized to be unpredictable and largely circular. See *infra* notes 159–61 and accompanying text. But so long as *Katz* governs the question of what qualifies as a search, that is the relevant standard. Moreover, to the extent that queries expose knowledge, the collection of which is already definitively recognized as a search, the indeterminate nature of the *Katz* inquiry itself does not pose a problem.

14. Recognizing a reasonable expectation of privacy in a database search is concededly a significant expansion of *Katz*'s reasonable expectation of privacy test, which to date has applied only to information collection. This expansion, however, is no more significant than the expansion of Fourth Amendment coverage that *Katz* itself represented at the time. See *infra* notes 187–93 and accompanying text.

15. This is not to say that collection reforms are not also important. I agree, for example, that the third-party doctrine should be curtailed. The point here is simply that if the concern comes from how the government is using information, reforming collection rules cannot alleviate that concern entirely.

than it used to;¹⁶ and (2) that the costs of storage and analysis have plummeted.¹⁷

Of course, the Constitution is not the only source of legal restrictions on government activity. Statutory, regulatory, policy-based, or judicially imposed constraints apply to use at times. Exactly what rules govern the collection and use of particular types of information vary, depending on both the nature of the data and the nature of the collection. When it comes to data regarding electronic communications, for example, non-content data (or metadata)—like call records or email routing information—currently lacks constitutional protection.¹⁸ But that data is subject to statutory constraints on its collection.¹⁹ The same is true for data such as financial and medical records. Even information that normally enjoys full Fourth Amendment protection under the warrant requirement, such as electronic communications, can sometimes be subject to a different regime. Thus when collecting electronic communications by targeting non-U.S. persons outside the United States for foreign intelligence purposes, which will inevitably collect the communications of U.S. persons as well—that collection need only be reasonable to satisfy the Constitution,²⁰ while more specific regulation comes from other sources.²¹ A patchwork of limits from disparate sources regulates the vast sea of data unrelated

16. Blood collected at a crime scene, for example, historically could only allow law enforcement to determine its type. Now that same sample can provide a detailed genetic profile. Sophisticated analysis of large volumes of data has similarly magnified the volume of knowledge that can be extracted from information. See Christopher Slobogin, *Government Data Mining and the Fourth Amendment*, 75 U. CHI. L. REV. 317 (2008) (discussing the expansion of the government's ability to analyze data about American citizens).

17. See *United States v. Jones*, 565 U.S. 400 (2012) (noting that technological advances enable greater police surveillance).

18. See *In re Application of the FBI for an Order Requiring the Production of Tangible Things from [REDACTED]* 9 (FISA Ct., Aug. 29, 2013) (holding that collection of bulk telephony metadata is not regulated by the Fourth Amendment).

19. See 50 U.S.C. § 1842(h)(1) (2012) (instructing the Attorney General to develop “appropriate policies and procedures” for protecting the privacy of “nonpublicly available information concerning United States persons”); USA FREEDOM Act of 2015, Pub. L. No. 114-23, §§ 201–202, 129 Stat. 268 (2015) (codified at 50 U.S.C. § 1861) (prohibiting bulk collection and instituting privacy procedures).

20. *In re Directives [REDACTED]* Pursuant to Section 105b of the Foreign Intelligence Surveillance Act, 551 F.3d 1004 (FISA Ct. Rev. 2008).

21. See *infra* notes 107–11 and accompanying text (discussing the nonconstitutional limits on government use of Americans' electronic communications captured in the courts of foreign intelligence surveillance).

to communications—social media postings; digital records of an individual's movements; and public records such as arrests, real estate purchases, or professional licenses.

Some commentators argue that these unconstitutional rules are the appropriate means to regulate the government's use of information.²² I disagree for a number of reasons.²³ First, if limits on information collection are any guide, nonconstitutional restrictions are often significantly less protective than Fourth Amendment-based regulation, frequently requiring only that the information is relevant to an ongoing investigation.²⁴ Second, Congress has been an unreliable actor in this area, legislating piecemeal—often in response to some form of scandal—rather than developing a comprehensive information privacy regime.²⁵ Similarly, internal or executive branch policy constraints generate a hodgepodge of rules, with different regulations applicable to different agencies, any of which may be modified at any time and are frequently secret. These are not qualities that generate sustained, meaningful privacy protections. Finally, the government is now capable of uncovering many of our most intimate details—things that historically might have been discoverable only by searching someone's “papers”²⁶—simply by manipulating data. Fourth Amendment doctrine must evolve to recognize some database queries as searches just as it has evolved over time in other ways to ad-

22. See, e.g., Orin S. Kerr, *Use Restrictions and the Future of Surveillance Law*, in THE FUTURE OF THE CONSTITUTION 3 (2011) (advocating for regulation of the entire surveillance process); William C. Banks, *Programmatic Surveillance and FISA: Of Needles and Haystacks*, 88 TEX. L. REV. 1633, 1637 (2010) (arguing for the development of a standardized system for authorized use of collected information); Solove, *A Taxonomy of Privacy*, *supra* note 10, at 521–22 (describing a framework through which to understand privacy). But see, Ric Simmons, *The Mirage of Use Restrictions*, 96 N.C.L. REV. (forthcoming 2017), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2937809 (reviewing use restrictions and discussing their justifications).

23. See *infra* Part III.C (discussing the need for constitutional regulation).

24. See, e.g., Christopher Slobogin, *Transaction Surveillance by the Government*, 75 MISS. L.J. 139, 149–67 (2005) (detailing the ease with which the government may collect call detail records, public records, medical records, credit information, stored communications, tangible things, and more); see also *infra* notes 251–52.

25. See *infra* notes 253–61 and accompanying text (discussing the insufficiency of legislative action).

26. The Fourth Amendment protects from unreasonable searches and seizures of people's “persons, houses, papers, and effects.” U.S. CONST. amend. IV.

dress challenges posed by new technology and new investigative techniques.²⁷

While my proposal would significantly expand the Fourth Amendment and may sound drastic, it is not as stark a divergence from existing doctrine as it may first appear. Indeed, my doctrinal approach builds on two existing strands of Fourth Amendment law. The first is a series of what I call collection-plus situations—circumstances in which collection is constitutionally permissible only when *paired* with postcollection use restrictions.²⁸ The Supreme Court has determined, for example, that foreign intelligence surveillance is consistent with the Fourth Amendment only when exercised in concert with “minimization procedures”—rules governing the government’s retention and dissemination of the fruits of that surveillance.²⁹ Imposing constitutional constraints on information use alone—as opposed to imposing them in conjunction with limits on particularly intrusive collection techniques—merely takes an additional step down that path.

The other strand of Fourth Amendment law on which I draw comes from the Supreme Court’s recent efforts to grapple with the powerful effects of information aggregation. *United States v. Jones* examined the scope of the government’s authority to engage in long-term warrantless GPS tracking. Black letter Fourth Amendment law provides that information identifying one’s location in a public space at any given moment is exempt from Fourth Amendment protection.³⁰ In *Jones*, however, the Court faced the question whether aggregating information about an individual’s precise location over the course of several weeks should lie similarly beyond the Constitution’s reach. In concurring opinions, five justices agreed that because such a “precise, comprehensive record of a person’s public movements” exposes “a wealth of detail about [that person’s] familial, political, professional, religious, and sexual associations,” it violates a reasonable expectation of privacy and should therefore be considered a search.³¹ In other words, the

27. See, e.g., Orin S. Kerr, *An Equilibrium-Adjustment Theory of the Fourth Amendment*, 125 HARV. L. REV. 476 (2011) (discussing how courts adjust Fourth Amendment doctrine in response to technology).

28. See *infra* notes 204–17 and accompanying text.

29. See *United States v. U.S. Dist. Court (Keith)*, 407 U.S. 297, 321 (1972); *Berger v. New York*, 388 U.S. 41, 58 (1967).

30. See *infra* notes 93–96 and accompanying text.

31. *United States v. Jones*, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring); see, e.g., *Riley v. California*, 134 S. Ct. 2473, 2492 (2014) (rejecting

aggregation of many pieces of data was simply too intrusive to go unregulated, even though the collection of any one piece of that data—the defendant’s location at any given moment—remained untouched by Fourth Amendment limits. When database queries about U.S. persons similarly reveal intimate knowledge discoverable only by aggregating multiple pieces of data, courts should consider those queries Fourth Amendment searches, regardless of how the data were collected.

Any objections to my proposal based on logistical concerns fail as well. The Foreign Intelligence Surveillance Court (FISC) has already provided a model for implementing these doctrinal changes in its own jurisprudence.³² As I have argued elsewhere, the FISC imposed constraints in the form of minimization procedures on the government’s Section 215 bulk telephony metadata program that approximated each of the Fourth Amendment warrant requirement’s elements.³³ And while the FISC did not explicitly rest these restrictions on constitutional foundations, its means of imposing *ex ante* review, as well as cause and particularity requirements, nevertheless provides a blueprint for what a Fourth Amendment use-restriction regime might look like.

This Article will proceed in three parts. Part I will first illustrate the incredible breadth and volume of information the government may collect. It will then demonstrate the threat to privacy that the power to aggregate that data poses. Part II turns to Fourth Amendment doctrine, first explaining how warrant requirement exceptions and Fourth Amendment exemptions remove much information collection from constraints traditionally applicable to searches and seizures and then exploring the powerful investigative tool this collection represents in light of the absence of use restrictions. In Part III, I will begin by making the case for treating as searches some database queries about U.S. persons. I will then show how the FISC’s jurisprudence provides a model for how this doctrinal shift might be implemented. Finally, I will explain why we

the warrantless search of an arrestee’s cell phone given the nature of the revelations made possible by searching smartphone contents); *see also Jones*, 565 U.S. at 419–31 (Alito, J., concurring).

32. The Foreign Intelligence Surveillance Court (FISC) is a federal court created by the Foreign Intelligence Surveillance Act of 1978 (FISA), 50 U.S.C. §§ 1801–1885(c) (2012) to review government applications to engage in domestic surveillance for foreign intelligence purposes. *Id.* § 1803(d).

33. Emily Berman, *Quasi-Constitutional Protections and Government Surveillance*, 2016 B.Y.U. L. REV. 771 (2016).

need constitutionally based use restrictions, rather than relying on statutory or regulatory rules. The Article will then briefly conclude.

I. COLLECTION AND AGGREGATION OF INFORMATION

This Part surveys the types of information the government collects about Americans and demonstrates that when the volume and variety of this information is combined with the government's analytical capacity "it is possible to learn far more than most people had anticipated."³⁴

A. THE INFORMATION THE GOVERNMENT CAN COLLECT³⁵

Most information the government collects does not implicate the Fourth Amendment at all. Information regarding immigration, social security benefits, military service, census information, and income tax is collected and stored in the course of everyday operations. Other sources of information are government audits, agency oversight activities, personnel hiring, and more. Many of these records will include information such as an individual's physical description, family history (marriages, divorces, children), place of residence, political activity, financial information, health care records (including medical conditions and use of prescription drugs), social security number, and beyond.³⁶ Statutes and regulations—rather than constitutional law—control government access to this type of information.

Of course, intelligence and law enforcement operations also engage in their own major collection operations. We learned with great fanfare in 2013 from the Edward Snowden leaks that the National Security Agency (NSA) had been collecting since 2006, bulk telephony metadata records—comprised of in-

34. John P. Holdren & Eric S. Lander, *Letter to President Barack Obama*, in *BIG DATA AND PRIVACY: A TECHNOLOGICAL PERSPECTIVE* (2014). One hint at the volume of information involved comes from the NSA's recent construction of a data storage facility roughly five times larger than the U.S. Capitol. James Bamford, *The NSA Is Building the Country's Biggest Spy Center (Watch What You Say)*, *WIRED* (Mar. 15, 2012), https://www.wired.com/2012/03/ff_nsadatacenter.

35. As this path has been well-trodden by others, this discussion will provide a broad overview. For more detailed discussion about government information collection, I commend to you the sources cited in notes 36–52, *infra*.

36. See Daniel J. Solove, *Access and Aggregation: Public Records, Privacy and the Constitution*, 86 MINN. L. REV. 1137, 1139 (2002) [hereinafter Solove, *Access and Aggregation*].

formation such the length of a call, the phone number from which the call was made, and the phone number dialed—produced by each telephone company regarding “all telephone calls made through its systems or using its services where one or both ends of the call are located in the United States.”³⁷ The revelation that, going back as far as 1987, the Drug Enforcement Administration (DEA) had “routine access” to similar information regarding “every call that passes through an AT&T switch—not just those made by AT&T customers”—drew less attention.³⁸ Call detail records are available to the government if they are “relevant and material to an ongoing criminal investigation.”³⁹ Law enforcement entities regularly seek other information from communications providers as well, notably cell site location information.⁴⁰ The Supreme Court granted certio-

37. *ACLU v. Clapper*, 785 F.3d 787, 796 (2d Cir. 2015). “Metadata can also reveal the user or device making or receiving a call through unique ‘identity numbers,’” as well as the routing of a call, which can indicate a caller’s general location. *Id.* at 793–94; *see also* ADMIN. WHITE PAPER, BULK COLLECTION OF TELEPHONY METADATA UNDER SECTION 215 OF THE USA PATRIOT ACT 3 (2013) (explaining the government’s legal basis for an intelligence collection program). Defining the line between content and metadata in the context of electronic communications has proved less than straightforward. *See, e.g., United States v. Warshak*, 631 F.3d 266 (6th Cir. 2010) (holding that e-mails constitute communications content protected by the Fourth Amendment); *United States v. Forrester*, 512 F.3d 500 (9th Cir. 2007) (finding that Internet Protocol addresses are noncontent metadata).

38. Scott Shane & Colin Moynihan, *Drug Agents Use Vast Phone Trove, Eclipsing N.S.A.’s*, N.Y. TIMES (Sept. 1, 2013), <http://www.nytimes.com/2013/09/02/us/drug-agents-use-vast-phone-trove-eclipsing-nsas.html>.

39. 18 U.S.C. § 2703(d) (2012).

40. Cell site location information (CSLI) is the compilation of data that cellular phones communicate with cell towers, conveying to cellular service providers details regarding the tower locations relied upon by users. According to AT&T, that company received 64,703 requests for such information in 2014; in the first half of 2015, Verizon received more than 21,000 such requests. Robinson Meyer, *Do Police Need a Warrant To See Where a Phone Is?*, ATLANTIC (Aug. 8, 2015), <https://www.theatlantic.com/technology/archive/2015/08/warrantless-cell-phone-location-tracking/400775>. For readers familiar with the podcast *Serial*, you may recall that much of the government’s case against Adnan Syed for the 1999 murder of Hae Min Lee came from CSLI, and much of the uncertainty regarding his guilt or innocence comes from debate regarding the accuracy and reliability of such records. *See Season One*, SERIAL, <https://serialpodcast.org/season-one> (last visited Nov. 5, 2017). For readers unfamiliar with *Serial*, do yourself a favor and listen to season one as soon as possible. Several circuits have determined that acquiring an individual’s historical CSLI is not a search and therefore does not require a warrant. *See, e.g., United States v. Graham*, 824 F.3d 421 (4th Cir. 2016) (en banc); *United States v. Carpenter*, 819 F.3d 880 (6th Cir. 2016); *United States v. Davis*, 785 F.3d 498 (11th Cir. 2015).

rari this Term to decide whether the warrantless collection of this kind of location information enjoys Fourth Amendment protection.⁴¹

Police forces and the FBI have an insatiable desire for data, and deploy a variety of sophisticated information collection tools to acquire it: cell tower simulators,⁴² automatic license-plate-recognition cameras—a technology designed to mark the location of a particular vehicle at a particular time⁴³—and a variety of surveillance cameras mounted on aerial drones,⁴⁴ in fixed locations, and on police cars and police officers.⁴⁵ Sophisticated means of conducting covert audio, video, and tracking surveillance are marketed to cities flush with counterterrorism funding.⁴⁶ The New York Police Department (NYPD) has

41. *Carpenter v. United States*, 137 S. Ct. 2211 (2017).

42. See, e.g., Nicky Woolf, *Stingray Documents Offer Rare Insight into Police and FBI Surveillance*, *GUARDIAN* (Aug. 26, 2016), <http://www.theguardian.com/us-news/2016/aug/26/stingray-oakland-police-fbi-surveillance> (discussing the FBI's use of cell site simulators).

43. See Cyrus Farivar, *Your Car, Tracked: The Rapid Rise of License Plate Readers*, *ARS TECHNICA* (Sept. 27, 2012), <https://arstechnica.com/tech-policy/2012/09/your-car-tracked-the-rapid-rise-of-license-plate-readers/>; Richard Read, *DEA Is Spying on Millions of U.S. Drivers with License Plate Readers*, *WASH. POST* (Jan. 27, 2015), http://www.washingtonpost.com/cars/dea-is-spying-on-millions-of-us-drivers-with-license-plate-readers/2015/01/27/96cb42c6-a644-11e4-a162-121d06ca77f1_story.html. The International Association of Chiefs of Police pointed out that automated license plate readers “may collect the license plate numbers of vehicles parked at locations that, even though public, might be considered sensitive, such as doctor’s offices, clinics, churches, and addiction counseling meetings, among others.” INT’L ASS’N OF CHIEFS OF POLICE, *PRIVACY IMPACT ASSESSMENT REP. FOR THE UTILIZATION OF LICENSE PLATE READERS* 21 (2009).

44. See Jack Gillum, et al., *FBI Behind Mysterious Surveillance Aircraft Over U.S. Cities*, *PBS* (June 2, 2015), <http://www.pbs.org/newshour/rundown/fbi-behind-mysterious-surveillance-aircraft-u-s-cities>.

45. See, e.g., William M. Bulkeley, *Chicago’s Camera Network Is Everywhere*, *WALL ST. J.* (Nov. 17, 2009), <https://www.wsj.com/articles/SB10001424052748704538404574539910412824756> (noting Chicago’s police department links its 1500 cameras with thousands of other cameras deployed by other government agencies and the private sector); Mike Carter, *Judge Blocks Seattle from Revealing Locations of FBI’s Hidden Cameras on Utility Poles*, *SEATTLE TIMES* (June 13, 2016), <https://www.seattletimes.com/seattle-news/crime/judge-blocks-seattle-city-light-from-disclosing-locations-of-fbi-surveillance-cameras>.

46. The tactical communications and surveillance catalog of British defense contractor Cobham was recently made public. It describes covert audio, video, and tracking surveillance equipment available to law enforcement agencies. *Product Quick Guide*, COBHAM TACTICAL COMM’NS & SURVEILLANCE (Feb. 2014), https://www.cobham.com/media/1078613/Cobham_TCS_QuickGuide_Mar14.pdf.

worked with Microsoft to develop what it calls domain awareness system (DAS), which aggregates in real time various data from the city's public surveillance cameras, arrest records, lists of completed crimes and their characteristics, vehicle tracking information collected from license plate readers, and more.⁴⁷ Moreover, agencies, at all levels of government, that collect data frequently share it both within the agency and externally to other government entities,⁴⁸ though the terms of the use of that data often remain shrouded from public view.⁴⁹

The government also acquires a great deal of information from the private sector. Some private-sector information comes from data-collection firms, such as ChoicePoint and Acxiom, that compile data from public records from around the country—information about births, marriages, divorces, property transactions, professional licenses, arrests, court proceedings, and more—and combine it with information from other sources, such as private detectives, as well as social media websites, property records, public health data, car rentals, utility bills, insurance claims, postal records, purchase history from discount and member-loyalty cards, and credit reporting firms, for sale to potential employers, landlords, and governments.⁵⁰ A

47. Joh, *supra* note 11, at 48–49; Press Release, Office of the Mayor, Mayor Bloomberg, Police Commissioner Kelly and Microsoft Unveil New, State-of-the-Art Law Enforcement Technology That Aggregates and Analyzes Existing Public Safety Data in Real Time To Provide a Comprehensive View of Potential Threats and Criminal Activity (Aug. 8, 2012), <http://www1.nyc.gov/office-of-the-mayor/news/291-12/mayor-bloomberg-police-commissioner-kelly-microsoft-new-state-of-the-art-law>. As of 2013, the NYPD had a database of sixteen million license plates, along with the data regarding where they were captured. *Id.* Microsoft is also marketing this technology to other cities; New York City will receive thirty percent of the proceeds from future sales. *Id.*

48. See, e.g., RACHEL LEVINSON-WALDMAN, BRENNAN CTR. FOR JUSTICE, WHAT THE GOVERNMENT DOES WITH AMERICANS' DATA 19–47 (2013), <https://www.brennancenter.org/sites/default/files/publications/Data%20Retention%20-%20FINAL.pdf>.

49. See, e.g., Larry Greenemeier, *What Is the Big Secret Surrounding Stingray Surveillance?*, SCI. AMERICAN (June 25, 2015), <https://www.scientificamerican.com/article/what-is-the-big-secret-surrounding-stingray-surveillance>.

50. David Gray & Danielle Citron, *The Right to Quantitative Privacy*, 98 MINN. L. REV. 62, 142 (2013); Slobogin, *supra* note 16, at 320; Solove, *Digital Dossiers*, *supra* note 8, at 1151 (discussing government contracts with such private firms). This flow of information from the private sector grows ever larger as the government encourages the development of “new information-gathering technologies.” See *Id.* at 1100. Information is big business. See Murphy, *supra* note 11 at 805–10 (2010) (discussing the history and current capacity of information databases); Solove, *Digital Dossiers*, *supra* note 8, at 1092

relatively new source of private-sector information is the Internet of Things—devices connected to the Internet that send and receive information—which allows the makers of products to track and record how they are used. Everything from thermostats to coffeemakers to baby monitors can be connected to the Internet, and information about those devices’ use can be captured in databases,⁵¹ the contents of which the government can then acquire.⁵²

Together, the information the government collects through routine activity, intelligence operations, law enforcement tools, and deals with private-sector data brokers a bewildering amount of information with little, if any, particularized basis.⁵³ To be sure, some of this data collection is valuable—necessary even. Imagine trying to redraw congressional districts without the census, or collecting taxes without information about individuals’ incomes. But this nonexhaustive list of the government’s contemporary data-collection potential should convey the enormity of both its volume and its breadth.

(“From credit reporting agencies, the government can glean information relating to financial transactions, debts, creditors, and checking accounts [as well as] details about people’s race, income, opinions, political beliefs, health, lifestyle, and purchasing habits from database companies.”); *id.* at 1084 (“In the Information Age, an increasing amount of personal information is contained in records maintained by Internet Service Providers (ISPs), phone companies, cable companies, merchants, bookstores, websites, hotels, landlords, employers and private sector entities.”). For evidence that information truly is big business, note that at one point ChoicePoint was valued at \$3.6 billion. *Reed Elsevier To Acquire ChoicePoint for \$3.6 Billion*, N.Y. TIMES (Feb. 21, 2008), <https://www.nytimes.com/2008/02/21/technology/21iht-reed.4.10279549.html>.

51. Bernard Marr, *Google’s Nest: Big Data and the Internet of Things in the Connected Home*, FORBES (Aug. 5, 2015), <https://www.forbes.com/sites/bernardmarr/2015/08/05/googles-nest-big-data-and-the-internet-of-things-in-the-connected-home/#6eb45273bac4>.

52. See Trevor Timm, *The Government Just Admitted It Will Use Smart Home Devices for Spying*, GUARDIAN (Feb 9, 2016), <https://www.theguardian.com/commentisfree/2016/feb/09/internet-of-things-smart-devices-spying-surveillance-us-government>. The same holds true for anything that conveys information about your movements and your purchases, such as items that contain a radio frequency identification (RFID) tag, which can include your passport, your credit card, your supermarket loyalty card, even the clothes that you wear. See Miguel Bustillo, *Wal-Mart Radio Tags To Track Clothing*, WALL ST. J., July 23, 2010, at A1; Alejandro Martinez-Cabrera, *Concern over Privacy As ID Tags’ Use Expands*, S.F. CHRON., Sept. 6, 2010, at D1 (reporting that a California county implanted RFID tags in preschoolers’ uniforms).

53. See Joh, *supra* note 11, at 39 (noting that ninety percent of the world’s data has been generated in the past two years, and that we now create as much information in two days as we did from the beginning of human civilization until 2003).

B. THE AGGREGATION PROBLEM

Though the volume and variety of information to which the government has access raises its own questions, my primary concern is what the combination (aggregation) of so much information enables the government to discover. Analysis can derive from data that private information, “at the time of their collection, seemed to raise no, or only manageable, privacy issues.”⁵⁴ Professor Solove has called this phenomenon the aggregation problem.⁵⁵ When seen “in isolation, each piece of our day-to-day information is not all that telling; viewed in combination, it begins to paint a portrait about” us.⁵⁶ The upshot is

54. PRES.’S COUNCIL OF ADVISORS ON SCI. & TECH., BIG DATA AND PRIVACY: A TECHNOLOGICAL PERSPECTIVE at ix (2014), https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/PCAST/pcast_big_data_and_privacy_-_may_2014.pdf [hereinafter PCAST].

55. Solove, *Access and Aggregation*, *supra* note 36, at 1185; *see also* Jack M. Balkin, *The Constitution in the National Surveillance State*, 93 MINN. L. REV. 1, 12 (2008) (noting that technologies allow the government “to record perfectly innocent behavior that no one is particularly ashamed of and draw from that data surprisingly powerful inferences about people’s behavior, beliefs, and attitudes”); Kate Crawford & Jason Schultz, *Big Data and Due Process: Toward a Framework To Redress Predictive Privacy Harms*, 55 B.C. L. REV. 93, 106 (2014) (“[O]ne cannot assess the predictive privacy risks from the collection of a single data point.”); Margaret Hu, *Small Data Surveillance v. Big Data Cybersurveillance*, 42 PEPP. L. REV. 773, 826 (2015) (discussing how a fusion of locational-body surveillance and biographical-behavioral surveillance allows the government to enable tracking and data analytics on potential suspects and/or terrorists); Solove, *Digital Dossiers*, *supra* note 8, at 1154 (“A fact here or there may seem innocuous but when combined, they become more telling about that person.”).

The aggregation problem is related to, but is distinct from, what has been labeled mosaic theory, which posits that “a series of acts that are not searches in isolation amount to a search when considered as a group.” *See* Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311, 320 (2012). The idea is that multiple nonsearches combined together may amount to a search because of the mosaic they reveal. *Id.* The quintessential example is the long-term surveillance of an individual’s public movements—combining a sufficient number of location data points over a sufficient period of time will reveal a great deal of information about the surveillance target’s life. While the mosaic theory describes one form of aggregation—the aggregation of information resulting from a series of government collection activities—it is focused on determining when a sequence of government acts constitutes a search. By contrast, I do not argue that a series of nonsearches becomes a search when a certain threshold is crossed. Instead, I argue that the single act of querying a database can itself be a search. *See infra* notes 221–24 and accompanying text.

56. Solove, *Access and Aggregation*, *supra* note 36, at 1185; *see also* PCAST, *supra* note 54, at x (noting that aggregating data “can result in the identification of individual people, the creation of profiles of an individual, and the tracking of an individual’s activities”).

that when government officials search—or query—aggregated information, they can learn a great deal more about the subject of the query than they could have done using any individual piece of data alone. Importantly, the additional information data aggregation provides may be “precisely the same information [the government] previously would have been required to obtain a warrant to access,” thereby undermining existing privacy protections.⁵⁷

Think of the aggregation problem as the difference between explicit and implicit knowledge.⁵⁸ Explicit knowledge is information that is plain on the face of data. Implicit knowledge is information that can be extracted through data analysis.⁵⁹ Consider the following hypothetical. Jane’s neighbor (or the license plate reader in her neighborhood) knows that, beginning two months ago, she started leaving for work one hour earlier on Thursday mornings than on other workdays; the grocery store clerk (or the grocery store’s member-loyalty program) knows that over that same time frame, Jane has eaten a pint of coffee ice cream every week; and the barista at a coffee shop on the other side of town (or the coffee shop’s frequent-customer program) knows that she recently became a Thursday morning regular.

Standing alone, each of these disclosures reveals only a small amount of information about Jane, none of which is particularly sensitive. But imagine that each of these facts was digitally stored in a government database, which investigators

57. TECH. & PRIVACY ADVISORY COMM., U.S. DEPT OF DEFENSE, SAFEGUARDING PRIVACY IN THE FIGHT AGAINST TERRORISM 36 (2004), <https://www.cdt.org/files/security/usapatriot/20040300tapac.pdf>.

58. K.A. Taipale, *Data Mining and Domestic Security: Connecting the Dots To Make Sense of Data*, 5 COLUM. SCI. & TECH. L. REV. 3, 37 (2003).

Extracting *implicit* information means that the results of data mining are not existing data items in the database. Traditional information retrieval from a database returns arrays consisting of data from individual fields of records (or entire records) from the database in response to a defined or specified database query. The results of the traditional database query are explicit in the database, that is, the answer returned to a query is itself a data item (or an array of many items) in the database. Data mining techniques, however, extract knowledge from the database that is implicit—knowledge that typically does not exist a priori is revealed.

Id. (internal citations and quotations omitted).

59. See *United States v. Jones*, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring) (noting that momentary location information is not particularly revealing, but aggregating location information can generate “a precise, comprehensive record” of a person’s life, reflecting “a wealth of detail about her familial, political, professional, religious, and sexual associations”).

can then query for all of the information it contains about Jane. The results of that query could easily lead to the conclusion (whether correct or incorrect) that something in Jane's life changed two months ago and that she now has a weekly Thursday morning appointment somewhere near a particular coffee shop. Further investigation into this Thursday morning activity could reveal regular trips to a psychiatrist, a fertility clinic, a substance abuse rehabilitation center, or any number of other intensely personal activities that neither a neighbor nor a barista could divine with the isolated bits of information available to them. In other words, querying a database compiled from disparate sources "reveals facts about data subjects in ways far beyond anything they expected" based on what they have revealed publicly.⁶⁰ The whole is more than the sum of its parts.

The threat posed by aggregation is not limited to hypotheticals. The NSA's post-9/11 surveillance programs illustrate the aggregation problem's implications. The now-discontinued Section 215 bulk telephone metadata surveillance program (named after the relevant statutory provision of the USA PATRIOT Act)⁶¹ involved collecting and aggregating all of Americans' telephony metadata, thereby compiling an enormous volume of Americans' telephone communications records.⁶² Government analysts could then query that database using a seed identifier, basically a search term (here, usually a phone number), to extract information regarding a particular individual.⁶³ A query yields "phone numbers, and the metadata associated with

60. Solove, *A Taxonomy of Privacy*, *supra* note 10, at 508; Solove, *Access and Aggregation*, *supra* note 36, at 1178 ("We know that our lives will remain private not in the sense that the information will be completely shielded from public access, but . . . because it is a needle in a haystack, and usually nobody will take the time to try to find it.").

61. USA PATRIOT Act of 2001, Pub. L. No. 107-56, § 215, 115 Stat. 272, 277-78 (2001) (codified as amended at 50 U.S.C. § 1861 (2012)) (permitting the FBI to "make an application for an order requiring the production of any tangible things . . . for an investigation to obtain foreign intelligence information . . . or to protect against international terrorism or clandestine intelligence activities"). The USA FREEDOM Act of 2015 eliminated the use of Section 215 for bulk collection. USA FREEDOM Act of 2015, Pub. L. No. 114-23, 129 Stat. 268 (2015) (codified at 50 U.S.C. § 1861).

62. PRIVACY & CIVIL LIBERTIES OVERSIGHT BD., REPORT ON THE TELEPHONE RECORDS PROGRAM CONDUCTED UNDER SECTION 215 OF THE USA PATRIOT ACT AND ON THE OPERATIONS OF THE FOREIGN INTELLIGENCE SURVEILLANCE COURT 8 (2014), https://www.pclob.gov/library/215-report_on_the_telephone_records_program.pdf [hereinafter PCLOB SECTION 215 REPORT].

63. *Id.* at 26-31.

them, that have been in contact with the seed.”⁶⁴ At that point, the government can then search for the numbers and associated metadata that have been in contact with the numbers the first query returns.⁶⁵ So rather than simply getting the list of numbers with which the seed is in contact, the aggregation of all metadata allows the government to map the entire communications network of the seed number.⁶⁶ Even conceding for the sake of argument that the collection of a single, targeted individual’s phone records does not raise privacy concerns,⁶⁷ the capabilities exercised in the Section 215 metadata program might give us pause. Indeed, it gave the American public pause when it came to light.⁶⁸

Section 702 of the Foreign Intelligence Surveillance Act (FISA) Amendments Act provides an even more troubling illustration, as that program authorizes the government to collect communications content,⁶⁹ which the Constitution has always treated as one of the most intrusive forms of surveillance.⁷⁰ The program collects the electronic communications into and out of the United States of a target “reasonably believed to be located outside the United States.”⁷¹ Electronic communications in-

64. *ACLU v. Clapper*, 785 F.3d 787, 797 (2d Cir. 2015).

65. *Id.*; PCLOB SECTION 215 REPORT, *supra* note 62, at 29 (“[Investigators are] able to view the records of calls involving telephone numbers that had contact with a telephone number that had contact with the original target.”).

66. Identifying unknown targets through scrutiny of an individual’s social networks is known as link analysis. Statement of Nathan A. Sales, Asst. Prof., George Mason Sch. of Law, PRIVACY & CIVIL LIBERTIES OVERSIGHT BD., WORKSHOP REGARDING SURVEILLANCE PROGRAMS OPERATED PURSUANT TO SECTION 215 OF THE USA PATRIOT ACT & SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT 2 (July 9, 2013).

67. This is the current state of the law according to the third-party doctrine. *See infra* notes 81–92 and accompanying text (discussing the third-party doctrine).

68. After the Section 215 program became public in 2013, President Obama slightly curtailed its scope; the USA FREEDOM ACT of 2015 then enacted several modifications, including a bar on bulk collection. *See* Jennifer Steinhauer & Jonathan Weisman, *U.S. Surveillance in Place Since 9/11 Is Sharply Limited*, N.Y. TIMES (June 2, 2015), <https://www.nytimes.com/2015/06/03/us/politics/senate-surveillance-bill-passes-hurdle-but-showdown-looms.html>.

69. 50 U.S.C. § 1881a (2012). Contrast this to the Section 215 program, which collected only metadata, which traditionally enjoys much less constitutional protection than content.

70. *See, e.g., Smith v. Maryland*, 442 U.S. 735, 741 (1979) (distinguishing a prior case which acquired the contents of a phone conversation from acquiring the number dialed).

71. 50 U.S.C. § 1881a(g)(2). Upon discovery that “a Section 702 target is a U.S. person or was inside the United States at the time of targeting, the gov-

cludes the contents of phone calls and email, as well as instant messages, Facebook messages, web browsing history, and Skype conversations.⁷² And while the government may neither target a U.S. person nor target a foreigner for the purpose of acquiring a particular U.S. person's communications, communications collected under this program necessarily include someone in the U.S.⁷³ This results, of course, in the collection of "a significant amount of information about U.S. persons."⁷⁴ Analysts may then query the database of Section 702—acquired information using a seed associated with a U.S. person, thus accessing any conversation that a particular U.S. person had with an overseas target.

The aggregation problem arises outside the foreign intelligence context as well. As Justice Sonia Sotomayor eloquently made plain in her concurrence in *United States v. Jones*, aggregating information about an individual's location over a substantial period of time generates "a wealth of detail about her familial, political, professional, religious, and sexual associations."⁷⁵ Investigators can extract location information by aggregating sufficiently extensive networks of cell tower simula-

ernment must stop the collection immediately," but is permitted to "waive" the general requirement that such communications must be destroyed. PRIVACY & CIVIL LIBERTIES OVERSIGHT BD., REPORT ON THE SURVEILLANCE PROGRAM OPERATED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT 127 (2014), <https://www.pclob.gov/library/702-report.pdf> [hereinafter PCLOB SECTION 702 REPORT].

72. See, e.g., Laura K. Donohue, *Section 702 and the Collection of International Telephone and Internet Content*, 38 HARV. J.L. & PUB. POL'Y 117, 120 (2015).

73. PCLOB SECTION 702 REPORT, *supra* note 71, at 127–33.

74. *Id.* at 133; see also Glenn Greenwald & Ewen MacAskill, *NSA Prism Program Taps in to User Data of Apple, Google and Others*, GUARDIAN (June 7, 2013), <http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data>.

75. *United States v. Jones*, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring). Similar information could be acquired by collecting CSLI in bulk. For a discussion of CSLI, see *supra* note 40. To date, no government agency has tried to acquire a comprehensive database of all CSLI (as far as I am aware), but a sufficient number of cell tower simulators deployed across a particular geographical area, would provide the same data. A query of a widely distributed network of automatic license plate readers (ALPR) fed into a single database regarding a particular individual's vehicle—a criminal suspect, an ex-girlfriend—would also return a map of that individual's movements. In a 2011 survey by the Police Executive Research Forum, seventy-one percent of responding agencies used ALPRs and eighty-five percent planned to acquire or increase their use over the next five years. POLICE EXEC. RESEARCH FORUM, *HOW ARE INNOVATIONS IN TECHNOLOGY TRANSFORMING POLICING?* 31 (2012), http://www.policeforum.org/assets/docs/Critical_Issues_Series/how%20are%20innovations%20in%20technology%20transforming%20policing%202012.pdf.

tors, surveillance cameras, automatic license plate reader (ALPR) technology, biometric information, or databases with records from companies such as E-Z pass, Travelocity, or Hotels.com.⁷⁶

You might wonder why we should be concerned about the information that the government collects and the kind of conclusions it can draw from aggregating and searching that information. After all, doesn't the Fourth Amendment protect our privacy? Wouldn't the Constitution bar the government's access to truly private information absent probable cause to believe criminal activity is afoot? As the next Part will make plain, the answer to both of these questions is an emphatic no.

II. FOURTH AMENDMENT LAW'S FAILURE

To fall within the Fourth Amendment's ambit, government action must qualify as a search or seizure. The current regime defining searches for Fourth Amendment purposes began in 1967, with *Katz v. United States*.⁷⁷ In *Katz*, the Supreme Court rejected the idea that the Fourth Amendment regulates only physical trespasses by government officials, holding that it protects "people, not places."⁷⁸ As a result, collecting the contents of a phone call made from a public telephone booth qualified as a search requiring a warrant.⁷⁹ Since *Katz*, the Fourth Amendment has regulated any government activity that violates an individual's reasonable expectation of privacy.⁸⁰

Such activity constitutes a search and must comply with constitutional limits. Usually those limits require the government to secure a warrant from a neutral magistrate based upon probable cause.

As Section A demonstrates, however, under contemporary doctrine, a great deal of information collection does not violate a reasonable expectation of privacy; even when it does, an exception to the warrant requirement often applies. Moreover,

76. The FBI's database of biometric information includes millions of photographs. U.S. GOV'T ACCOUNTABILITY OFFICE, FACE RECOGNITION TECHNOLOGY: FBI SHOULD BETTER ENSURE PRIVACY AND ACCURACY 10 (2016), <https://www.gao.gov/assets/680/677098.pdf>. This database is used by both federal and state investigators. *Id.* at 11.

77. 389 U.S. 347 (1967). Prior to *Katz*, the Fourth Amendment regulated government activity that physically invaded protected spaces, like houses or offices. *Id.* at 352–53.

78. *Id.* at 351.

79. *Id.* at 353.

80. *Id.* at 361 (Harlan, J., concurring).

the absence of constitutional limits regarding the government's use of that information, as Section B will explain, magnifies any concerns raised by the dearth of Fourth Amendment limits on collection. Section C will then demonstrate how recent Supreme Court cases reveal the tension that the power of information aggregation is currently creating within Fourth Amendment doctrine.

A. THE FOURTH AMENDMENT'S PERMISSIVE INFORMATION COLLECTION RULES

This Section discusses two circumstances in which the warrant requirement does not apply. First, what I call Fourth Amendment *exemptions* refer to instances in which the collection at issue does not qualify as a search or seizure. The Supreme Court's interpretation of *Katz's* reasonable-expectation-of-privacy test places an enormous amount of information—some of it highly sensitive—in this category. Second, I refer to instances where the Fourth Amendment applies but the government need not secure a warrant as warrant requirement *exceptions*. In those circumstances, the government action must merely be reasonable, a determination courts make by balancing the government's interest in collection against the intrusiveness of the search or seizure. This Section will show how these exemptions and exceptions often swallow the Fourth Amendment rule.

Three preliminary points are in order. First, this Section does not provide an exhaustive catalog of Fourth Amendment exceptions and exemptions. It should, however, illustrate the permissiveness of the overall regime. Second, in this Article I take no position in the heated, long-running debate regarding the appropriate scope of existing exemptions and exceptions. Instead, I simply expound existing doctrine. Third, I recognize that the collection of information that enjoys no Fourth Amendment protection may nevertheless be subject to statutory or regulatory limits. As I explain in Part III, *infra*, I find those types of limits unsatisfactory as a general matter; moreover, even with the most stringent collection rules, the aggregation problem would still present a privacy threat.

1. Fourth Amendment Exemptions

Of the numerous Fourth Amendment exemptions, those responsible for most of the investigative activity relevant to the aggregation problem come from one of two doctrines. First is

the third-party doctrine, by far the most significant Fourth Amendment exemption.⁸¹ The doctrine provides that any information we voluntarily reveal to a third party—a term encompassing any individual or nongovernmental institution—enjoys no Fourth Amendment protection.⁸² In *Smith v. Maryland*, one of the doctrine's foundational cases, the Supreme Court held that law enforcement's collection of the list of phone numbers that a criminal suspect dialed did not constitute a search because the suspect should have reasonably expected that his telecommunications provider kept track of such information and he had therefore voluntarily relinquished it.⁸³ By relinquishing this information to another, the doctrine reasons, one cedes any reasonable expectation of privacy in it.⁸⁴

Consider what is included in this category of information: phone records identifying who you associate with; bank records showing who you do business with; credit card records revealing where you eat, shop, and seek entertainment; medical records listing your prescriptions; the records of cable companies and video-streaming services exposing what you watch; Internet browsing history indicating whether you have searched for symptoms of disease or investigated substance abuse treatment options; and travel records from airlines, hotels, rental car companies, or other third parties like Orbitz or Kayak.⁸⁵ The third-party doctrine also denies Fourth Amendment protections to information that private firms gather from your appliances.⁸⁶

81. The third-party doctrine has never been well loved by commentators, and members of the academy continue to produce suggestions to eliminate or modify it. See, e.g., Kerr, *supra* note 8, at 563–64 nn.5–11 (compiling a list of critiques of third-party doctrine); Peter P. Swire, *Katz Is Dead. Long Live Katz.*, 102 MICH. L. REV. 904 (2004); see also sources cited *supra* note 8.

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

83. *Maryland*, 442 U.S. at 743–45.

84. *Id.*

85. See Solove, *Digital Dossiers*, *supra* note 8, at 1090–91.

86. *Id.* A particularly aggressive interpretation of the third-party doctrine was also used to justify the NSA's warrantless bulk collection of telephone metadata. Under that program, rather than simply collecting the call records of a particular individual, as it had done in *Smith*, the government collected all of the telephony metadata recorded by communications providers of all calls made through their system where one or both ends of the communication were in the United States. *ACLU v. Clapper*, 785 F.3d 787, 795–99 (2d Cir. 2015); see also *supra* notes 70–85 and accompanying text, *infra* notes 87–110 and accompanying text. And, because both the government and the FISC agreed that telephone metadata qualified as third-party records that are not

To be sure, some of the data subject to collection under the third-party doctrine is subject to statutory or policy-based rules. To collect an individual's communications metadata under Section 215, for example, the government must certify that the "information likely to be obtained" is "relevant to an ongoing investigation to protect against international terrorism or clandestine intelligence activities."⁸⁷ And the Attorney General must "include privacy protections that apply to the collection, retention, and use of information concerning United States persons."⁸⁸ Medical records also enjoy statutory protection.⁸⁹ But as privacy scholars have demonstrated repeatedly, the existing legal framework for protecting individual privacy is, on the whole, outdated and incomplete.⁹⁰

Note that the principle behind the third-party doctrine—the idea that anything you have voluntarily provided to a third party lacks Fourth Amendment protection—is not limited to written records. The third-party doctrine's close cousin, sometimes referred to as the "false friend" doctrine, applies the same idea to spoken conversations.⁹¹ There is no reasonable expectation of privacy in what someone voluntarily tells an interlocutor, even if—unknown to the speaker—she happens to be a government agent or informant.⁹² This doctrine allows law enforcement or intelligence officials to attend and record (or task informants to attend and record) religious or political gather-

entitled to Fourth Amendment protection, the government was able to assemble a vast database made up of an enormous volume of Americans' telephone communications records, both domestic and international, with no constitutionally imposed limits. Amended Memorandum Opinion at 3, *In re Application of FBI for an Order Requiring the Prod. of Tangible Things from [REDACTED]*, No. BR 13-109 (FISA Ct., Aug. 29, 2013).

87. 50 U.S.C. § 1842(c)(2) (2012). Metadata collected in the criminal context must be "relevant to an ongoing criminal investigation." 18 U.S.C. § 3122(b)(2) (2012).

88. 50 U.S.C. § 1842(h)(1).

89. Slobogin, *supra* note 24, at 158.

90. See, e.g., 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. 1208, 1233 (2004) (noting that one particular privacy statute is "vague in some places, overly complex in others, and underprotective of privacy interests in others"); Slobogin, *supra* note 24, at 149–67 (describing limited privacy protections for information other than communications content); Daniel J. Solove & Chris Jay Hoofnagle, *A Model Regime of Privacy Protection*, 2006 U. ILL. L. REV. 357, 364–68 (2006) (describing the "limits of U.S. privacy law"); see sources cited *infra* notes 251–52.

91. Paul Ohm, *The Fourth Amendment in a World Without Privacy*, 81 MISS. L.J. 1309, 1326 (2012).

92. *E.g.*, *Hoffa v. United States*, 385 U.S. 293, 296 (1966).

ings as well as individual conversations.

While the third-party doctrine is the most noteworthy Fourth Amendment exemption, another is also quite significant. The Supreme Court held in *Knotts v. United States* that when government officials collect information about one's physical location in a public place—even if aided by an electronic tracking device—that collection is neither a search nor a seizure.⁹³ The Court reasoned that people “traveling in an automobile on public thoroughfares” voluntarily convey the details of their travels “to anyone who want[s] to look.”⁹⁴ Under a broad reading of *Knotts*, the government could argue that the Fourth Amendment does not apply to any location-tracking method so long as the government has not trespassed on private property to collect the information.⁹⁵ Cell site location information (CSLI) gathered through the use of a cell tower simulator or from a communications provider,⁹⁶ video surveillance paired with facial-recognition software, toll records, or license plate readers all can be viewed simply as a means of collecting location information. So long as the resulting data is limited to locations in public places, *Knotts* arguably permits such acquisition as merely the gathering of information voluntarily divulged to the public at large. Regulations addressing these forms of collection, if they exist, vary from jurisdiction to jurisdiction.⁹⁷

2. Warrant Requirement Exceptions

In circumstances where the Fourth Amendment applies but the warrant requirement does not, the traditional limits of ex ante review, probable cause, and particularity become fall away. In these cases, the Fourth Amendment merely requires that, taking into account the totality of the circumstances, the government search or seizure is “reasonable.” Courts determine

93. *United States v. Knotts*, 460 U.S. 276, 282 (1983); *see also* *United States v. Karo*, 468 U.S. 705 (1984) (holding that the use of a beeper to track a person's location was not a search under the Fourth Amendment until the beeper entered a home).

94. *Knotts*, 460 U.S. at 281–82; *cf. Karo*, 468 U.S. at 731–32 (holding that the Fourth Amendment is only violated by the warrantless location search of a container at the moment it enters a private home).

95. *See* *United States v. Jones*, 565 U.S. 400, 414 (2012) (Sotomayor, J., concurring).

96. For information on CSLI's constitutional status, *see* discussion *supra* note 40.

97. Solove & Hoofnagle, *supra* note 90, at 380–82.

whether government action is reasonable by balancing the government's interest against the intrusiveness of the search; reasonableness sometimes, but not always, requires individualized suspicion.⁹⁸

The most important warrant requirement exception for the purposes of this Article is the foreign-intelligence-surveillance exception.⁹⁹ Under this exception, the government need not secure a warrant to collect information with foreign intelligence value.¹⁰⁰ In *In re Directives*, the Foreign Intelligence Surveillance Court of Review (FISCR)¹⁰¹ held that, "a foreign intelligence exception to the Fourth Amendment's warrant requirement exists when surveillance is conducted to obtain foreign intelligence for national security purposes and is directed against [targets] reasonably believed to be located outside the United States."¹⁰² The FISCR also found the surveillance pro-

98. See, e.g., *Terry v. Ohio*, 392 U.S. 1, 30 (1968) (holding stop-and-frisk searches permissible with reasonable suspicion that the person is "armed and presently dangerous"); *Warden v. Hayden*, 387 U.S. 294, 298–300 (1967) (creating an "exigent circumstances exception" to the warrant requirement for home searches); *Carroll v. United States*, 267 U.S. 132, 153 (1925) (allowing for warrantless search of vehicles with reasonable suspicion of crime); see also *California v. Carney*, 471 U.S. 386, 393–95 (1985) (extending vehicle exception to mobile homes in certain circumstances).

99. The foreign intelligence surveillance exception is actually just one application of a broader warrant requirement exception known as the special needs doctrine. That doctrine provides that a warrantless search may be justified when special needs, "beyond the normal need for law enforcement," make the warrant and probable-cause requirements of the Fourth Amendment impracticable. E.g., *New Jersey v. T.L.O.*, 469 U.S. 325, 351 (1985) (Blackmun, J., concurring). Under this rationale, the Supreme Court has approved as consistent with the Fourth Amendment: (1) the U.S. Customs' Service's mandatory drug testing of employees seeking promotion to positions involving interdiction of illegal drugs, requiring them to carry firearms, or requiring them to handle classified materials; (2) a school district's random drug testing for student athletes; (3) the search of a probationer's home; and (4) numerous other contexts. *Vernonia Sch. Dist. 47J v. Acton*, 515 U.S. 646 (1995); *Nat'l Treasury Emps. Union v. Von Raab*, 489 U.S. 656, 665–66 (1989); *Griffin v. Wisconsin*, 483 U.S. 868, 873, 875 (1987). See also *Bd. of Educ. of Indep. Sch. Dist. No. 92 v. Earls*, 536 U.S. 822 (2002) (holding that individualized suspicion is not required to justify random drug testing of students involved in extracurricular activities); *Skinner v. Ry. Labor Execs.' Ass'n*, 489 U.S. 602 (1989) (holding that warrantless drug and alcohol tests for railway employees were reasonable even in the absence of reasonable suspicion that any particular employee was impaired).

100. *T.L.O.*, 469 U.S. at 336.

101. FISA created a Court of Review (FISCR), made up of three federal district or appeals court judges appointed by the Chief Justice, to hear appeals from decisions of the FISC. 50 U.S.C. § 1803 (2012).

102. *In re Directives*, 551 F.3d 1004, 1012 (FISA Ct. Rev. 2008). *In re Direc-*

gram as a whole reasonable and therefore lawful under the Fourth Amendment.¹⁰³

This case gave a green light to the Section 702 program's collection of non-U.S. persons' electronic communications, so long as the target is "reasonably believed to be located outside the United States."¹⁰⁴ If the government directly targeted U.S. persons for their international electronic communications, such surveillance would indisputably require individualized probable cause.¹⁰⁵ Yet because the program both qualifies for the foreign-intelligence-surveillance exception to the warrant requirement and has been deemed reasonable by the FISC, the Fourth Amendment poses no obstacle to this collection—even in the absence of individualized suspicion about the overseas target's American interlocutors.¹⁰⁶

As with communications metadata, Section 702 collection and the use of the resulting data are subject to some statutory, policy-based, and judicially imposed limits.¹⁰⁷ For example, a "significant purpose" of the collection must be to gather foreign intelligence information—a relatively expansive category¹⁰⁸—

tives involved a challenge to the temporary Protect America Act (PAA), Pub. L. No. 110-55, § 105B, 121 Stat. 552 (2007). The PAA was replaced in 2008 by the FISA Amendments Act (FAA), Pub. L. No. 110-261 (codified at 50 U.S.C. §§ 1881a–g).

103. *In re Directives*, 551 F.3d at 1012–15. The FISC held that the surveillance met the Fourth Amendment's reasonableness requirement in light of the government's interest in protecting national security and the "matrix of safeguards" that mitigated the intrusiveness of the program. *Id.*

104. *Id.* See 50 U.S.C. § 1881a(g)(2).

105. *United States v. U.S. Dist. Court (Keith)*, 407 U.S. 297 (1972); 50 U.S.C. §§ 1801–1805.

106. *In re Directives* implied that an executive order requiring the Attorney General to have probable cause to believe that the targeted person is a foreign power or its agent was one of several constitutionally compelled procedural protections. *In re Directives*, 551 F.3d at 1014.

107. See, e.g., 50 U.S.C. §§ 1861, 1881a; ERIC H. HOLDER, JR., ATT'Y GEN. OF U.S., PROCEDURES USED BY THE NSA FOR TARGETING NON-UNITED STATES PERSONS REASONABLY BELIEVED TO BE LOCATED OUTSIDE THE UNITED STATES (2009) (detailing NSA targeting procedures); Berman, *supra* note 33, at 806–17 (detailing the judicially imposed limits on Section 215 and Section 702 data); Peter Margulies, *Reauthorizing the FISA Amendments Act: A Blueprint for Enhancing Privacy Protections and Preserving Foreign Intelligence Capabilities*, 12 J. BUS. & TECH. L. 23, 37–39 (2016) (describing judicially and executive-branch-imposed limits on data collection).

108. See 50 U.S.C. § 1801(e). A target of Section 702 surveillance "could be completely innocent." *Hearing on Oversight and Reauthorization of the FISA Amendments Act: The Balance Between National Security, Privacy and Civil Liberties Before the S. Comm. on the Judiciary*, 114th Cong. 7 (2016) (statement of David Medine, Chairman, Privacy and Civil Liberties Oversight

but it need not be the only purpose.¹⁰⁹ Indeed the primary purpose of the collection could be something totally unrelated—such as a criminal investigation.¹¹⁰ And while queries of the Section 702–acquired information are themselves subject to rules developed in conjunction with the FISA,¹¹¹ those rules do not prevent the most troubling practice (from a Fourth Amendment perspective, anyway): analysts may perform so-called U.S. person queries, which ask for communications involving a particular U.S. person. Such a query returns all international communications that U.S. person engaged in with any overseas target, regardless of its foreign intelligence value.¹¹² This occurs despite the statute barring the targeting of U.S. persons for collection.¹¹³

Other courts have relied on the foreign-intelligence-surveillance exception to bless the warrantless search of a U.S. citizen's home in Kenya¹¹⁴ as well as New York City's suspicionless searches of individuals riding the subway.¹¹⁵ The list of warrant requirement exceptions is long—it includes searches or seizures of items in plain view, border searches,¹¹⁶ inventory searches, consent searches, and more.¹¹⁷

Board). For an argument that a broad definition of “foreign intelligence information” is necessary to successful diplomacy, see Peter Margulies, *Defining “Foreign Affairs” in Section 702 of the FISA Amendments Act: The Virtues and Deficits of Post-Snowden Dialogue on U.S. Surveillance Policy*, 72 WASH. & LEE L. REV. 1283, 1283–87 (2015).

109. 50 U.S.C. § 1881a(g)(2)(A)(v).

110. The NSA determines who will be targeted, but the FBI may “nominate” targets. PCLOB SECTION 702 REPORT, *supra* note 71, at 47.

111. See NAT'L SEC. AGENCY, U.S. SIGNALS INTELLIGENCE DIRECTIVE, USSID SP0018, LEGAL COMPLIANCE AND U.S. PERSONS MINIMIZATION PROCEDURES § 4 (2011); NAT'L SEC. AGENCY, MINIMIZATION PROCEDURES USED BY THE NSA IN CONNECTION WITH ACQUISITIONS OF FOREIGN INTELLIGENCE INFORMATION PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT § 3 (2007); William C. Banks, *Next Generation Foreign Intelligence Surveillance Law: Renewing 702*, 51 U. RICH. L. REV. 671, 672–88 (2017) (detailing nonconstitutional limits on Section 702 data collection and use).

112. In 2016, the government (not including the FBI, which is exempt from reporting requirements) used 5288 search terms associated with a U.S. person. OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, STATISTICAL TRANSPARENCY REPORT REGARDING USE OF NATIONAL SECURITY AUTHORITIES FOR CALENDAR YEAR 2016, at 8 (2017).

113. *In re Directives*, 551 F.3d 1004, 1012–15 (FISA Ct. Rev. 2008).

114. *In re Terrorist Bombings of U.S. Embassies in E. Afr.*, 552 F.3d 93 (2d Cir. 2008).

115. *MacWade v. Kelly*, 460 F.3d 260 (2d Cir. 2006) (permitting application of the special needs exception to a warrantless search where the subject of a search possesses a full privacy expectation).

116. See *United States v. Ramsey*, 431 U.S. 606, 616 (1977) (finding that

This brief discussion of a couple of those exceptions, however, shows that the default Fourth Amendment rule requiring a showing of probable cause, identification of the object of the search or seizure with particularity, and *ex ante* approval by a neutral magistrate does not always apply. In fact, there are many circumstances in which the government constitutionally may collect large swaths of information about Americans without satisfying one or more of the traditional Fourth Amendment limits, and often without any individualized suspicion at all.

B. THE FOURTH AMENDMENT'S (NON)EXISTING USE-RESTRICTION RULES

The government's broad collection rules plainly raise their own privacy concerns, but even if they did not, postcollection use would still pose such threats. Indeed, the government's broad collection power might not be so alarming if there were reliable limits on how the government used the information in its possession. As this Section will demonstrate, however, the conventional wisdom is that once data is in the government's hands, the Constitution has nothing to say at all.¹¹⁸ In the

routine searches of people and their effects at the border are "reasonable simply by virtue of the fact that they occur at the border"). The advent of digital storage devices, such as laptops, cell phones, and thumb drives, has generated numerous questions regarding the application of the border search doctrine to the contents of these devices. The Supreme Court has not yet weighed in on the issue, but courts addressing the question have consistently held that routine inspection of electronic media—which would include booting up a device, reviewing its contents, and using search functions to find and review specific files—is permissible, even in the absence of suspicion. *See, e.g.*, *United States v. Saboonchi*, 990 F. Supp. 2d 536, 549 (D. Md. 2014); *United States v. Ickes*, 393 F.3d 501, 502–03 (4th Cir. 2005). The rule is slightly less permissive when it comes to forensic border searches, which generally entail making a mirror of the entire contents of the digital device, and then subjecting that copy to scrutiny using analytic software to recover hidden, deleted, or encrypted data. *See Saboonchi*, 990 F. Supp. 2d at 547–48. To engage in forensic searches, the government must have individualized suspicion, which is not a particularly high bar. *Id.* at 570 ("This standard is far from onerous.").

117. *See Investigations and Police Practices—Warrantless Searches and Seizures*, 44 GEO. L.J. ANN. REV. CRIM. PROC. 48 (2015) (listing additional exceptions to the warrant requirement).

118. *E.g.*, *United States v. Comprehensive Drug Testing, Inc.*, 621 F.3d 1162, 1173 (9th Cir. 2010) ("It goes without saying that lawfully seized evidence may not be suppressed."); *Boroian v. Mueller*, 616 F.3d 60, 67–68 (1st Cir. 2010) (retaining a former offender's DNA profile "does not constitute a separate search under the Fourth Amendment"); *see also Balkin, supra* note 55, at 20 ("[B]ecause the Fourth Amendment focuses on searches and seizures, it places few limits on collation and analysis."); *Joh, supra* note 11, at 63 ("If

words of one respected jurist, “the [F]ourth [A]mendment does not control how properly collected information is deployed.”¹¹⁹

Whatever logic this constitutional vacuum may have had in the past, the absence of use restrictions cannot persist in the face of the convergence of two factors. First, there remains very little information about what we do, where we go, what we purchase, or with whom we communicate that some third party does not record and store digitally. This means the government will have access to an ever-growing amount of information about each individual American. Similarly, we now live in a networked world. Many Americans have family, friends, or business associates all around the globe. With international communications ubiquitous and—so long as you can find a Wi-Fi connection—free, long distance phone charges are a thing of the past. Moreover, much of this international interaction takes place through modes of communication—e-mails, instant messages, video and voice chats, videos, photos, voice-over-IP (such as Skype or FaceTime), and other digital tools—that are subject to collection under the Section 702 program.¹²⁰ Accordingly, a great deal more of our communications are likely vulnerable to collection.

Second, contemporary technology permits the government to collect, store, aggregate, and analyze large volumes of data in ways that were either unavailable or cost prohibitive for most of America’s history.¹²¹ So even as we generate more and more digital information about ourselves, the government’s ca-

[information] acquisition is permissible, how the police use that information thereafter is generally not subject to an additional Fourth Amendment challenge.”); Kerr, *supra* note 22, at 6 (“If the government comes across information legally, then it is free to use that information however officials would like.”); Erin Murphy, *Back to the Future: The Curious Case of United States v. Jones*, 10 OHIO ST. J. CRIM. L. 325, 330–31 (2012) (“Current Fourth Amendment law emphasizes acquisition It cares little for what happens next—to what use that information is put.”); William J. Stuntz, *O.J. Simpson, Bill Clinton, and the Transsubstantive Fourth Amendment*, 114 HARV. L. REV. 842, 857 (2001) (“Fourth Amendment law regulates the government’s efforts to uncover information, but it says *nothing* about what the government may do with the information it uncovers.”).

119. *Green v. Berge*, 354 F.3d 675, 680 (7th Cir. 2004) (Easterbrook, J., concurring).

120. *Greenwald & MacAskill*, *supra* note 74; *see also supra* notes 70–110 and accompanying text (describing the Section 702 program).

121. *See generally* Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801 (2004) (discussing the impact of changing technologies on Fourth Amendment doctrine).

capacity for exploiting that information grows.¹²² Thanks to contemporary technology, government information collection and analysis powers have grown substantially in recent decades. And while over time there have been some technology-driven changes to constitutional rules regarding government collection, the rules (or lack of them) when it comes to information use have remained stagnant.

C. THE FOURTH AMENDMENT IN THE DIGITAL AGE

Two recent Supreme Court cases starkly illustrate the pressure that modern technology places on existing Fourth Amendment doctrine. In *United States v. Jones* and *Riley v. California*, the Supreme Court recognized the transformative nature of data aggregation and considered whether current doctrine needs to be modified in response.¹²³ *United States v. Jones* presented almost exactly the same question that *Knotts* considered nearly three decades earlier—whether tracking a vehicle’s location on public thoroughfares over time constitutes a search¹²⁴—a question that *Knotts* answered in the negative.¹²⁵ *Jones* presented the issue, however, in a more technologically sophisticated context: whether law enforcement had engaged in an unlawful search when it placed a GPS device on a suspect’s car without a valid warrant and used it to collect a detailed account of his movements over the course of several weeks.

122. Solove, *A Taxonomy of Privacy*, *supra* note 10, at 497 (comparing an automobile tracking device to the historic practice of police following a defendant on a highway or street).

123. The need for Fourth Amendment doctrine to accommodate technological change did not suddenly arise for the first time in the twenty-first century. Doctrine began grappling with technology’s effects by at least the 1920s. In *United States v. Lee*, 274 U.S. 559, 563 (1927), for example, the Supreme Court held that the Coast Guard did not engage in a search when it used a searchlight to illuminate otherwise hidden cases of alcohol on a boat during the Prohibition Era. *See also* *Kyllo v. United States*, 533 U.S. 27, 40 (2001) (holding that the use of a thermal imaging device to monitor the radiation of heat from a home is a search). Throughout American history, as investigative methods have evolved, courts have continuously recalibrated the doctrine, sometimes announcing new rules, sometimes simply explaining how the old rules applied to new contexts. *See, e.g.*, *Katz v. United States*, 389 U.S. 347, 352–53 (1967); *see also* *Kerr*, *supra* note 27, at 531 (explaining how courts adjust Fourth Amendment doctrine in response to technology to maintain the balance of power between would-be criminals and the government).

124. *United States v. Jones*, 565 U.S. 400, 402 (2012).

125. *United States v. Knotts*, 460 U.S. 276, 282 (1983); *see also supra* notes 93–95 and accompanying text.

While the *Jones* majority opinion rested its holding that this *did* constitute a search on the decidedly nontechnological fact that government officials “physically occupied private property” when they placed the GPS device on Jones’s car,¹²⁶ two concurrences (representing five justices) recognized that the case implicated larger questions about how the Fourth Amendment should approach technological advances. Justice Alito argued that long-term GPS surveillance violates a reasonable expectation of privacy.¹²⁷ Justice Sotomayor explained how several technological factors have combined to change the nature—and hence the intrusiveness—of location information since the Court decided *Knotts*.¹²⁸ Contemporary monitoring tools provide a much more detailed, complete set of data,¹²⁹ and are much more likely to be used because they are cheap and invisible.¹³⁰ Justice Alito made a similar point when observing that, “[i]n the precomputer 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.”¹³¹ Moreover, Sotomayor pointed out, once collected, the government can “store such records and efficiently mine them for information years into the future.”¹³² As a result, Justice Sotomayor concluded, such collection is fundamentally *different in kind* from physical surveillance aided by a beeper like the one in

126. See *Jones*, 565 U.S. at 404.

127. *Id.* at 430–31 (Alito, J., concurring).

128. *Id.* at 414 (Sotomayor, J., concurring).

129. *Id.* at 414–16 (noting the extensive personal information that use of GPS devices can generate, including “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”).

130. *Id.* at 416 (quoting *Illinois v. Lidster*, 540 U.S. 419, 426 (2004)) (noting the low cost and minimal manpower required for GPS surveillance allow the government to evade “the ordinary checks that constrain abusive law enforcement practices: ‘limited police resources and community hostility’”); see also *Jones*, 565 U.S. at 429–30 (Alito, J., concurring) (arguing that historically the most effective privacy protections were practical rather than constitutional or statutory and that the monitoring at issue in *Jones* “would have required a large team of agents, multiple vehicles, and perhaps aerial assistance,” a use of resources that would only have been limited to “investigation[s] of unusual importance”); Kevin S. Bankston & Ashkan Soltani, *Tiny Constables and the Cost of Surveillance: Making Cents out of* *United States v. Jones*, 123 YALE L.J. ONLINE 335, 341–50 (2014).

131. *Jones*, 565 U.S. at 429 (Alito, J., concurring).

132. *Id.* at 415 (Sotomayor, J., concurring).

Knotts.¹³³ Courts must “take these attributes,” she argues, “into account when considering the existence of a reasonable societal expectation of privacy in the sum of one’s public movements.”¹³⁴

To be sure, the government might obtain the exact same information through analog surveillance techniques as it could via long-term GPS monitoring.¹³⁵ But this does not mean that GPS monitoring poses the same level of intrusion as conventional surveillance. For most of our history, practical impediments precluded law enforcement from collecting the information captured by GPS devices. Law enforcement is unlikely to invest the resources required to follow someone like Jones, who was suspected of possession with the intent to distribute cocaine, twenty-four hours a day for several weeks. Moreover, due to these practical constraints, courts never had to face the question whether months-long twenty-four-hour surveillance constituted a search. Hence Justice Sotomayor’s conclusion that the surveillance at issue in *Jones* presented a novel question not controlled by short-term surveillance cases like *Knotts*. In eliminating these practical obstacles to physical surveillance, technological advances do not only permit more collection. More importantly, the volume of collection amounts to an entirely new sort of surveillance: the results of aggregating that data, enabling the government to extract knowledge (intimate details about our daily lives, activities, and relationships) in which we have always had a reasonable expectation of privacy. Now that technology has eliminated the practical obstacle to aggregating large amounts of location information, the courts must erect a doctrinal bulwark to protect that expectation of privacy.

In other words, certain technology, when combined with storage and analysis capacity, raises the aggregation problem in a way that implicates reasonable expectations of privacy. At least five members of the Court recognized the distinction between government access to information revealed piecemeal (an individual’s location in public at any given moment in time) and access to an extensive dossier assembled by aggregating many isolated pieces of information (the compilation of weeks of information about Jones’s vehicle’s location).¹³⁶ The D.C. Cir-

133. *Id.*

134. *Id.* at 416.

135. *Id.* at 415.

136. See *id.* at 413, 418 (Sotomayor, J., concurring and Alito, J., concurring).

cuit Court's Judge Ginsburg perhaps put it best when he explained in the lower court's opinion in *Jones* that,

It is one thing for a passerby to observe or even to follow someone during a single journey as he goes to the market or returns home from work. It is another thing entirely for that stranger to pick up the scent again the next day and the day after that, week in and week out, dogging his prey until he has identified all the places, people, amusements, and chores that make up that person's hitherto private routine.¹³⁷

So while we may have no reasonable expectation of privacy in one piece of information about our location in public, the calculus regarding long-term GPS surveillance is different, given the conclusions one can draw from the aggregation of location information spanning several weeks.

In *Riley v. California*, the Supreme Court also acknowledged the potential intrusiveness facilitated by modern technology's ability to aggregate large amounts of information.¹³⁸ *Riley* presented the question whether law enforcement officials may, without a warrant, search the digital information contained on a smartphone seized in a search incident to arrest.¹³⁹ In searching David Riley upon his arrest for driving on a suspended license, the arresting officer found Riley's smartphone in his pocket and looked through it, discovering evidence that Riley had gang connections.¹⁴⁰ The Court had to decide whether the information gleaned from the cell phone was lawfully collected or whether its collection exceeded the scope of the search-incident-to-arrest warrant exception.¹⁴¹

Again, the Court—this time in an opinion joined by all nine justices—took the broader view of the Fourth Amendment's protections, pointing to the ways in which new technology changed the analysis on which the search-incident-to-arrest doctrine relied. While smartphones like Riley's were unheard of ten years ago, the Court noted, "a significant majority of American adults now own such phones."¹⁴² Moreover, these phones

137. *United States v. Maynard*, 615 F.3d 544, 560 (D.C. Cir. 2010), *aff'd sub nom. United States v. Jones*, 565 U.S. 400 (2012).

138. *Riley v. California*, 134 S. Ct. 2473, 2485 (2014).

139. Searches incident to arrest, in which an arresting officer may search the arrestee's person and immediate surroundings to ensure the preservation of evidence and officer safety, are a recognized exception to the warrant requirement. *See Arizona v. Gant*, 556 U.S. 332, 338 (2009) (acknowledging the permissible scope of such searches has long been a source of debate).

140. *Riley*, 134 S. Ct. at 2480.

141. *Id.*

142. *Id.* at 2484.

grant access to “vast quantities of personal information.”¹⁴³ So while “a mechanical application” of doctrine “might well support the warrantless search,” the Court determined that such an application was inappropriate when it comes to smartphones.¹⁴⁴ Permitting such devices to be searched with no warrant would pose a significantly greater intrusion into individual privacy than a traditional search incident to arrest of the nondigital contents of one’s pockets.¹⁴⁵

As with GPS-generated location data, the privacy implications of smartphone data distinguishes it from familiar pre-smartphone contexts not only in volume but also in the nature of the information.¹⁴⁶ A phone with Internet access will have search and browsing history, which could reveal an individual’s private interests or concerns—“perhaps a search for certain symptoms of disease, coupled with frequent visits to WebMD.”¹⁴⁷ Given the nature of the revelations that searches of smartphone contents permit, the Court determined that individuals have a reasonable expectation of privacy in those contents, even in the course of a valid search incident to arrest.¹⁴⁸

Less recently, the Supreme Court explicitly recognized the ability of data aggregation to exacerbate privacy concerns in the Freedom of Information Act (FOIA) context.¹⁴⁹ *United States Department of Justice v. Reporters Committee for Freedom of the Press* considered a request under FOIA for a particular individual’s criminal record.¹⁵⁰ The Court rejected the request, holding that even though criminal records are publicly available, disclosing a complete rap sheet would be an unwarranted invasion of personal privacy.¹⁵¹ The Court noted that, “there is a vast difference between the public records that might be found after a diligent search of courthouse files, coun-

143. *Id.* at 2484–85; *see also id.* at 2488 (equating a search of all data stored on a cell phone to a search of an arrestee’s wallet or purse was “like saying a ride on horseback is materially indistinguishable from a flight to the moon” because both are ways to get “from point A to point B, but little else justifies lumping them together”).

144. *Id.* at 2484.

145. *Id.* at 2488–89.

146. *Id.* at 2489.

147. *Id.* at 2490.

148. *Id.* at 2493.

149. Freedom of Information Act, Pub. L. No. 89-487, 80 Stat. 250 (1966) (as amended).

150. *U.S. Dep’t of Justice v. Reporters Comm. for Freedom of Press*, 489 U.S. 749 (1989).

151. *Id.* at 763–70.

ty archives, and local police stations throughout the country and a computerized summary located in a single clearinghouse of information.”¹⁵² As a result, it reasoned, there is a distinction “between scattered disclosure of the bits of information contained in a rap sheet and revelation of the rap sheet as a whole.”¹⁵³

As these cases show, the Supreme Court has already begun to recognize that doctrine must account for the government’s technology-enabled ability to glean new kinds of knowledge. Both *Jones* and *Riley*, as well as commentators’ suggestions for reforms,¹⁵⁴ however, remain focused on the proper scope of *collection*, trying to calibrate what should be available to the government in the first place. I suggest below that rather than (or in addition to) modifying collection rules, courts should employ *use* restrictions, subjecting some uses of even lawfully collected information to independent Fourth Amendment regulation.

The critical point here is that revelations that the government can glean by querying these databases are different in kind from revelations gleaned by collection alone. That is to say, more data is not necessarily *just* more data. More data can mean *different* data. The aggregation problem means that the right combination of multiple pieces of data can reveal data of an entirely novel—and much more sensitive—nature. So while basic information routinely revealed to the public at large (like momentary location information) may lack constitutional significance, five Supreme Court Justices have indicated that the government’s ability to build an individual’s profile beyond the scope of what law enforcement agencies would acquire in the absence of the ability to aggregate presents a distinct question.¹⁵⁵

III. TREATING QUERIES AS SEARCHES

This Article argues that the best way to address the aggregation problem is to reject the idea that the Constitution should remain indifferent to information use. Instead, doctrine should acknowledge that some postcollection and aggregation uses of information qualify as Fourth Amendment events in their own

152. *Id.* at 763–64.

153. *Id.*

154. *See supra* sources cited in note 8.

155. Benjamin J. Priester, *Five Answers and Three Questions After United States v. Jones (2012), the Fourth Amendment “GPS Case,”* 65 OKLA. L. REV. 491, 522 (2013).

right. This Part makes the case that some queries of aggregated databases for information about U.S. persons constitute such a use. Section A argues that there some queries violate reasonable expectations of privacy just as surely as some physical searches do, and that those queries should be regulated as searches.¹⁵⁶ Section B offers a means to implement this suggestion by demonstrating that the FISA Court has provided a model for such regulation. Finally, Section C discusses why use restrictions must derive from the Constitution, rather than from statutory or regulatory sources.

Before turning to my argument, however, a clarification is in order: there is a distinction between analyzing large data sets in search of patterns—what is typically referred to as data mining—and querying a data set for information about a particular U.S. person.¹⁵⁷ Retrieving information using query-and-report tools identifies what responsive bits of information a database contains about a specific individual, whereas data mining uses automated processes to discover patterns within the data. My argument applies only to queries. There may be instances when data mining is sufficiently invasive that it, too, should be considered a search; that, however, is a question for another paper.¹⁵⁸

A. WHY (AT LEAST SOME) QUERIES ARE SEARCHES

As noted above, courts determine what qualifies as a Fourth Amendment search by employing the inquiry first announced in Justice Harlan’s seminal concurrence in *Katz v. United States*, which instructs that the Fourth Amendment

156. I take no position here on *how* these searches should be regulated—i.e., whether they should require probable cause and warrants or whether some less demanding standard of review, such as reasonable suspicion, would be appropriate.

157. Data mining is the “process of identifying valid, novel, potentially useful and ultimately understandable patterns in data” or “the application of database technology and techniques—such as statistical analysis and modeling—to uncover hidden patterns” 1 WAYNE R. LAFAVE, *SEARCH AND SEIZURE: A TREATISE ON THE FOURTH AMENDMENT* § 2.7(e) (5th ed. 2012) (citations and internal quotations omitted); *see also* Taipale, *supra* note 58, at 37–39 (2003) (noting the difference between data aggregation analyzed with subject-based queries and the use of actual data mining).

158. Imagine, for example, that an algorithm identifies the following pattern: individuals who have both attended services at a mosque and traveled to South Asia are more likely to access terrorist propaganda online. It is not clear whether extracting a list of names of individuals who meet that pattern is any less invasive than a query about a specific individual. I hope to explore this and related questions about other forms of data use in future work.

regulates government activity when it violates an individual's "reasonable expectation of privacy."¹⁵⁹ Like the third-party doctrine, the reasonable-expectation-of-privacy test is subjected to its fair share of criticism, due in large part to its indeterminacy—it is often impossible to divine *ex ante* whether a court will find that a given set of facts violates a reasonable expectation of privacy.¹⁶⁰ Determining which expectations of privacy are reasonable is therefore more art than science.¹⁶¹ Yet *Katz* remains the law of the land.

In this Section, I argue that, at the very least, a query constitutes a search if it returns information whose exposure clearly would qualify as a search if that exposure was achieved by collection rather than query. In other words, when queries result in revelations that the Supreme Court has held would violate an expectation of privacy if achieved through collection, that query is a search. In such cases, the reasonable expectation of privacy is no less violated because it was accomplished through a query rather than a more traditional search.

159. *Katz v. United States*, 389 U.S. 347, 360–61 (1967) (Harlan, J., concurring).

160. For a representative catalogue of the scholarly critiques of the reasonable-expectation-of-privacy test, see William Baude & James Y. Stern, *The Positive Law Model of the Fourth Amendment*, 129 HARV. L. REV. 1821, 1825 n.7 (2016) (collecting articles critiquing the test as ambiguous, subjective, unpredictable, conceptually confused, and circular). As the leading treatise on searches and seizures puts it, the Supreme Court in *Katz* rejected the then-existing, arguably outmoded, Fourth Amendment principles while offering "little to fill the void" it had created. LAFAVE, *supra* note 157 § 2.1(a) ("The Supreme Court . . . has never managed to set out a comprehensive definition of the word 'searches' as it is used in the Fourth Amendment."); see also Anthony G. Amsterdam, *Perspectives on the Fourth Amendment*, 58 MINN. L. REV. 349, 403 (1974) (arguing that the question whether something is a search is "a value judgment" regarding how much "privacy and freedom" may be diminished by government surveillance before the Constitution imposes restraints); Orin S. Kerr, *Four Models of Fourth Amendment Protection*, 60 STAN. L. REV. 503, 504 (2007) ("[N]o one seems to know what makes an expectation of privacy constitutionally 'reasonable.'").

161. Of course the Supreme Court has made clear that some collection activities definitively constitute a search. See, e.g., *Kyllo v. United States*, 533 U.S. 27, 40 (2001) (finding that the examination of interior of private home with thermal imaging sensor was a search). Conversely, others definitively do not. See, e.g., *California v. Greenwood*, 486 U.S. 35, 37 (1988) (holding that police examination of contents of an individual's trash left at the curb for collection was not a search); *California v. Ciraolo*, 476 U.S. 207, 215 (1986) (holding that police surveillance of private property from a plane in navigable airspace was not a search). For cases that present novel facts, the Supreme Court's eventual outcome is often unclear. See *supra* notes 81–92 and accompanying text (discussing the third-party doctrine).

When queries return information whose collection by other means arguably violates a reasonable expectation of privacy, but the courts have not yet determined whether those means constitute a search, the question becomes more difficult. The government's acquisition of long-term location information about an individual provides a good example. Case law does not clearly indicate whether this acquisition violates a reasonable expectation of privacy and therefore constitutes a search. A query that returns long-term location information by aggregating information from multiple sources—say CSLI, license plate reader records, toll records, and facial recognition paired with surveillance camera footage—therefore may or may not qualify as a search, depending on how the Supreme Court ultimately decides the question. When faced with knowledge acquired by query whose independent collection does not violate a clearly established reasonable expectation of privacy, courts must simply engage in the same analysis that they perform when faced with a new form of collection. They will have to apply the *Katz* test, and make a judgment regarding whether the exposure of that information should be labeled a search. While this leaves uncertainty regarding which queries are permitted, the same is true of new collection methods until the courts resolve their status. When it comes to CSLI, for example, the government has implemented a policy of seeking warrants out of an abundance of caution while we await the Supreme Court's ruling. It could take the same approach to queries whose status is uncertain.

Queries of Section 702—acquired information using U.S. person identifiers present a stark example of the first type of query.¹⁶² Americans unquestionably have a reasonable expectation of privacy in the contents of our electronic communications and to collect them directly the government must first obtain ex ante judicial approval, based on probable cause, in the form of a warrant or a FISC order.¹⁶³ Queries seeking U.S. person information in Section 702—acquired information—which includes a “potentially very large” volume of “communications between lawful targets and U.S. persons that are not the type of com-

162. For a description of the Section 702 program, see *supra* notes 70–110 and accompanying text.

163. 50 U.S.C. § 1804 (2012) (discussing foreign intelligence investigations); 18 U.S.C. § 2518 (discussing criminal investigations).

munications Section 702 was not designed to collect”¹⁶⁴ that may “include family photographs, love letters, personal financial matters, discussions of physical and mental health, and political and religious exchanges”¹⁶⁵—can yield this normally constitutionally protected data with no individualized suspicion, particularity, or ex ante judicial approval.¹⁶⁶ The government thus may “use queries to digitally compile the entire body of communications” associated with an individual, even if that individual is a U.S. person.¹⁶⁷ And in fact, the FBI’s internal regulations permit exactly that.¹⁶⁸ Such queries have actually come to be known as the Fourth Amendment’s backdoor loophole, because they arguably serve as an end-run around the Fourth Amendment itself.¹⁶⁹ While information about the extent to which the government takes advantage of this “loop-hole” is imperfect,¹⁷⁰ a FISC judge discouraged Congress from

164. Brief of Amicus Curiae at 11, [Redacted] (FISA Ct., Oct. 16, 2015); see also Transcript of Proceedings Held Before the Honorable Thomas F. Hogan at 5–6, *In re* [Redacted] (FISA Ct., Oct. 20, 2015) (arguing that the FBI’s rules regarding Section 702 queries “do not provide sufficient safeguards of the U.S. Person information that” Section 702 collects).

165. *Hearing on Oversight and Reauthorization of the FISA Amendments Act: The Balance Between National Security, Privacy and Civil Liberties Before the S. Comm. on the Judiciary*, 114th Cong. 7 (2016) (statement of David Medine, Chairman, Privacy and Civil Liberties Oversight Board).

166. Professor Laura Donohue has argued that, when used to search for violations of the criminal law, queries of Section 702–acquired material should be considered searches requiring a warrant. Donohue, *supra* note 72, at 262–63.

167. PCLOB SECTION 702 REPORT, *supra* note 71, at 131; see also *id.* at 127 (noting that the privacy implications of Section 702 are not limited to collection, “but must also consider how information about U.S. persons is treated after collection”).

168. Memorandum Opinion & Order at 44, [Redacted] (FISA Ct., Nov. 6, 2015).

169. See, e.g., Elizabeth Goitein, *The FBI’s Warrantless Surveillance Back Door Just Opened a Little Wider*, JUSTSECURITY (Apr. 21, 2016), <https://www.justsecurity.org/30699/fbis-warrantless-surveillance-door-opened-wider>. A recent FISC opinion reached the opposite conclusion, determining that queries using U.S. person identifiers did not render the Section 702 program unreasonable for Fourth Amendment purposes. Memorandum Opinion & Order at 77, [Redacted] (FISA Ct., Nov. 6, 2015).

170. PCLOB SECTION 702 REPORT, *supra* note 71, at 130–31 (noting that the FBI “does not separately designate [queries] that employ U.S. person identifiers, and so the number of [such] queries performed by the FBI is not known” making “the manner in which the FBI is employing U.S. person queries . . . difficult to evaluate”).

requiring ex ante authorization for such queries because they are so common that the requests would swamp the court.¹⁷¹

It is less certain whether the type of query at issue in the Section 215 telephony metadata program or the GPS tracking in *Jones* violates a reasonable expectation of privacy. These types of cases of course present difficult line-drawing challenges.¹⁷² In the Section 215 program, the government (1) collected the metadata of all Americans' phone calls (metadata not subject to Fourth Amendment protections because the government secured it from a third party); (2) combined that metadata into a single database; and (3) then queried that database in search of as-yet-unknown terrorist operatives in the United States.¹⁷³ Without the capacity to aggregate these records, the government could acquire Individual X's phone records and learn all of the phone numbers with which Individual X communicates.¹⁷⁴ If the government wanted to know more about the communications of people who use the numbers with which Individual X is in contact, however, it would have to request individually the records associated with each of the numbers Individual X called or from whom Individual X received a call. And if it wanted more information about the numbers with which those numbers were in contact, it would have to do the same thing again. A conservative estimate says that two such "hops" would require the government to seek and review records associated with at least 10,000 phone numbers.¹⁷⁵ And if the government expanded the inquiry to three hops, the applicable rule for most of the Section 215 program's history, that number would rise to around 2.5 million.¹⁷⁶ Just as law enforcement is unlikely to follow Mr. Jones's car twenty-four hours a day for several weeks running, intelligence officials are unlikely to un-

171. Letter from Hon. John D. Bates, Dir., Admin. Office of U.S. Courts, to Sen. Dianne Feinstein, Chair, U.S. Senate Select Comm. on Intelligence, at 2 (Jan. 13, 2014).

172. See Simmons, *supra* note 22, at 7–8.

173. PCLOB SECTION 215 REPORT, *supra* note 62, at 21–31 (explaining access procedures for foreign intelligence and international terrorism investigations subject to Section 215).

174. *Id.* Section 215 requires only that the information sought be relevant to an ongoing investigation.

175. Klayman v. Obama, 957 F. Supp. 2d 1, 31 (D.D.C. 2013), *vacated and remanded*, 800 F.3d 559 (D.C. Cir. 2015) (containing the estimate cited by the court).

176. Noa Yachot, *Writers, Lawmakers, and the NRA Support ACLU Challenge to NSA Spying*, ACLU (Sept. 4, 2013), <https://www.aclu.org/blog/national-security/writers-lawmakers-and-nra-support-aclu-challenge-nsa-spying>.

dertake this chore on the off chance that they will spot a connection to a known terrorist.

Given a database that includes everyone's phone records, however, one query using Individual X's phone number would return all numbers within the specified number of hops.¹⁷⁷ In one mouse click, the government can discover not only the list of individuals and institutions who were recipients or originators of Individual X's phone calls, but also generate a map of their entire communications network and the networks of everyone with whom they is in contact.¹⁷⁸ Thus, even if we voluntarily relinquish our phone records to our communications provider, as the third-party doctrine assumes, the ability to map our entire social and professional network and what the government may learn from it is far more intrusive than simply gathering a list of numbers with which one person was in contact. Just as five justices believed that using a GPS tracking device to combine data available to the government in unaggregated form violated a reasonable expectation of privacy,¹⁷⁹ so too might this creation of an electronic rolodex violate an individual's expectations of privacy, even if the collection of each individual set of phone records does not.¹⁸⁰ In cases like this, it will not always be clear *ex ante* when a query will be considered a search. But the same is true of any application of the *Katz* test to novel circumstances.¹⁸¹

177. In part for this reason, when Congress renewed Section 215 in the USA FREEDOM ACT of 2015, it barred the government from amassing databases through the bulk collection of records. USA FREEDOM Act of 2015, Pub. L. No. 114-23, 129 Stat. 268 (2015) (codified at 50 U.S.C. § 1861).

178. See *supra* note 161 (referring to a graphics interchange format (GIF) with map showing hops).

179. See *supra* notes 127–29 and accompanying text.

180. One district court implicitly accepted this premise when arguing that the bulk metadata program did not present the same Fourth Amendment question as that of third-party-records cases like *Smith v. Maryland* and should not qualify for the third-party-records Fourth Amendment exemption. *Klayman*, 957 F. Supp. 2d at 31.

181. See Kerr, *supra* note 160, at 503 (describing the difficulty in anticipating what constitutes a search under *Katz* as having “disappointed scholars and frustrated students for four decades”). Indeed, judges have reached contrasting conclusions on the question whether the collection aspect of Section 215 constituted a search. Compare *Klayman*, 957 F. Supp. 2d at 31 (holding that bulk telephony metadata should not qualify for the third-party exemption), with *In re Application of the FBI for an Order Requiring the Prod. of Tangible Things from [Redacted]* (FISA Ct., Aug. 25, 2013) (holding that the third-party doctrine applies to bulk telephony metadata).

The issue of aggregating location data provides another example. In *Jones*, several of the justices believed the surveillance violated a reasonable expectation of privacy, and yet the Court did not settle the question whether extended GPS surveillance constitutes a search in the absence of a physical trespass.¹⁸² The Fourth Amendment status of the collection of CSLI remains similarly unsettled.¹⁸³ Or imagine a database of all the information gathered by a citywide network of license plate readers. The government could query that database for all cars that ran the red light at the intersection of Main and Broadway. Such a query seems to fall under the *Knotts* rule because it is isolated information about a vehicle's location in a public place.¹⁸⁴ But the government also could query that database for all instances in which it captured the license plate of Jane's vehicle. Like the GPS device in *Jones*, that query could reveal many of the private details of Jane's everyday life by identifying the places that Jane frequents. Just as the *Jones* surveillance arguably violates a reasonable expectation of privacy, so too might the query of the license-plate-reader data. Such queries do not clearly fall on one side of the reasonable-expectation-of-privacy line or the other. Eventually, however, appeals courts will reach a consensus on these specific issues, or the Supreme Court will announce a rule. There is no reason this form of rulemaking, so central to our common law system, cannot be applied to database queries in the same way it is applied to novel questions about information collection.

Another potential objection to this approach is, how will an analyst know, prior to running a query, what information it will return? Since the Fourth Amendment status rests on the nature of the information that the query reveals, rather than the nature of the query itself, it might seem to demand that analysts have a crystal ball enabling them to anticipate whether any particular query will qualify as a search. While this is not an insignificant concern, it can be addressed in a couple of ways. First, there will be times when an analyst running a query will know for sure that the query should be treated as a search. Any query of a database that includes Americans' communications content will, necessarily, implicate a reasonable expectation of privacy. Second, there will be times when an an-

182. See *supra* notes 124–37 and accompanying text (discussing the *Jones* majority and concurrences).

183. See *supra* note 40 (defining CSLI and citing cases).

184. See *supra* notes 93–94 and accompanying text (discussing *Knotts*).

alist will not know for certain that her query will return Fourth Amendment protected knowledge, but will have a sense—based on the nature of the data being queried as well as the reason for running the query—whether the resulting knowledge will categorize the query as a search. A query of a database with comprehensive historical location data, for example, can be expected to reveal intimate details of the query subject's life akin to those revealed by GPS surveillance in *Jones*.¹⁸⁵ Over time, as the nature of information that certain sets of databases return, it might become much clearer ex ante when a reasonable expectation of privacy is at stake. Finally, it may be that this uncertainty can be captured in the substantive rules that apply to queries that qualify as searches. For example, perhaps such queries qualify as an exception to the warrant requirement, and so the analyst's decision to query must simply be reasonable.¹⁸⁶ Under such a regime, any query that unexpectedly returns information protected by a reasonable expectation of privacy might be considered reasonable nonetheless. Just as the existing application of the reasonable-expectation-of-privacy test presents difficult and often hard-to-predict line-drawing exercises on the part of law enforcement and the courts, so too will determining when queries must be treated as searches (and what limits should be placed on such searches). But just as this has not prevented Fourth Amendment doctrine regarding collection to develop, the same could prove true in the context of information use, such as queries.

To be sure, this rule represents a significant change in conceptualizing the protective scope of the Fourth Amendment. And yet it is no more significant a change than *Katz* itself represented. Prior to *Katz*, *Olmstead v. United States* governed what qualified as a search.¹⁸⁷ Under the *Olmstead* regime, the government did not engage in a search unless it physically intruded into a "constitutionally protected area."¹⁸⁸ Thus in *Olmstead*, installing a tap on telephone wires "did not amount to a search . . . within the meaning of the Fourth Amendment," because the wires themselves were not located in a constitu-

185. See generally *supra* note 98 (discussing the results of the GPS surveillance in *Jones*).

186. See *supra* note 98 (defining reasonableness as an exception to the warrant requirement).

187. 277 U.S. 438 (1928).

188. *E.g.*, *Berger v. New York*, 388 U.S. 41, 44 (1967).

tionally protected area, like Olmstead's home or office.¹⁸⁹ Over time, however, the Court "departed from the narrow view on which [*Olmstead*] rested," and, finally, in *Katz* explicitly rejected the "constitutionally protected area" formulation in favor of inquiring into "what [an individual] seeks to preserve as private, even in an area accessible to the public."¹⁹⁰ And so was born the reasonable-expectation-of-privacy test.¹⁹¹

In rejecting the *Olmstead* approach, the *Katz* majority noted that, "[t]o read the Constitution more narrowly is to ignore the vital role that the public telephone has come to play in private communication."¹⁹² Similarly, to refuse to acknowledge the expectation of privacy Americans have in the results of some queries is to ignore the technological changes in how information is stored, transferred, collected, and analyzed. If, as *Katz* declared, "the Fourth Amendment protects people, not places,"¹⁹³ it should protect them against violations of their reasonable expectations of privacy regardless of the means by which that violation is accomplished. Justice Harlan declared in his *Katz* concurrence that "reasonable expectations of privacy may be defeated by electronic as well as physical invasion."¹⁹⁴ If a wiretap that reveals "what [an individual] seeks to preserve as private" is a search, then a query that exposes that same information represents just as significant an intrusion.¹⁹⁵

Regulating queries as searches also makes more sense than trying to address this issue by reforming collection rules. To be sure, one can argue that Fourth Amendment harm occurs the moment the government collects information about an individual. When it comes to the type of collection at issue here, we tend to retain our anonymity at the point of collection. Information about our spending or travel habits, or even the content of our Google chats, may be sitting on the government's servers, but nobody is looking at them. To the extent the goal is barring arbitrary government action to protect each individual from unreasonable intrusion into his or her zone of privacy, the moment government action becomes problematic is when it singles

189. 277 U.S. at 466.

190. *Katz v. United States*, 389 U.S. 347, 352–53 (1967).

191. *Id.*

192. *Id.* at 352.

193. *Id.* at 351.

194. *Id.* at 362 (Harlan, J. concurring).

195. *Id.*

out an individual for scrutiny.¹⁹⁶ Once the government has a particular individual in its sights, it can extract details from the vast ocean of data about that person. And it is at that moment—when the government generates a detailed profile about you from a sea of aggregated data—that Fourth Amendment rules barring arbitrary intrusive action should apply. If we worry about the government extracting information about specific individuals, then the concern manifests itself at the moment of extraction. Addressing the concern at its source also allows us to protect individual rights while continuing valuable collection programs.

There are also technological barriers to relying on collection rules to do all the work. As the President's Council of Advisors on Science and Technology pointed out, data sometimes contains "latent information about individuals," which is revealed only if exposed to certain forms of analysis.¹⁹⁷ One cannot regulate the collection of data one cannot see. Moreover, the aggregation of multiple data points from one form of collection (such as location data) can itself pose problems. Only limiting or eliminating government collection of all location information would address this issue through collection regulation. Finally, it is often impossible to know whether any given data point will reveal intimate knowledge when combined with other data either already in the government's possession or collected subsequently.¹⁹⁸

A final objection might be that queries hold too much value as an investigative tool to subject to Fourth Amendment limits. Just because some queries constitute searches, however, does not mean government investigators cannot perform them. As the courts often remind us, "the 'touchstone' of the Fourth

196. Solove, *A Taxonomy of Privacy*, *supra* note 10, at 489–90 (recognizing that harms from information use are distinct from those caused by collection). Not only is the collection of large datasets less troubling from an individual rights perspective, it can also be quite valuable. *See, e.g.*, U.S. GEN. ACCOUNTING OFFICE, DATA MINING: FEDERAL EFFORTS COVER A WIDE RANGE OF USES 2–3 (2004) (finding that the government uses data mining to improve service or performance, detect fraud, waste, and abuse; analyze scientific and research information; detect criminal activity, analyze intelligence and detect terrorist activities).

197. PCAST, *supra* note 54, at 39; *see also id.* at x–xi ("[A] policy focus on limiting data collection will not be a broadly applicable or scalable strategy—nor one likely to achieve the right balance between beneficial results and unintended negative consequences (such as inhibiting economic growth).").

198. *See id.* at 47–48.

Amendment is reasonableness.”¹⁹⁹ Just because a query qualifies as a search does not mean the government must secure a warrant based on probable cause. Perhaps it makes sense to include queries in the list of warrant requirement exceptions, such that an analyst running a query must have probable cause to do so but need not secure ex ante judicial sign-off. Or perhaps the courts will consider queries to be more like *Terry* stops,²⁰⁰ requiring only reasonable suspicion. Courts in this context must be asked to balance the government’s interest in law enforcement against society’s interests in individual rights, just as they do in so many other places.

B. OPERATIONALIZING QUERY-SEARCHES

Having determined that some database queries are searches—referred to hereafter as query-searches²⁰¹—how can we ensure that the government carries them out in a manner consistent with the Fourth Amendment? To answer this question, this Section first demonstrates that expanding Fourth Amendment protections to some information use is not as radical a departure from existing doctrine as it first might appear. It then details how the FISC has already provided a roadmap for how Fourth Amendment limitations can be imposed on database query-searches.

1. The Foundation for Constitutionally Based Use Restrictions

While the Constitution is silent on the government’s use of information in the lion’s share of circumstances,²⁰² the Fourth Amendment does, in fact, require more than the traditional constitutional protections governing searches and seizures in a handful of situations. Both Congress and the courts consider some information collection methods so intrusive that postcollection constraints on information use are necessary.²⁰³ So, in some ways recognizing queries as potential searches merely expands existing doctrine rather than contradicting it.

199. *E.g.*, *Ohio v. Robinette*, 519 U.S. 33, 39 (1996).

200. *See supra* note 98 and accompanying text (discussing *Terry v. Ohio*, 392 U.S. 1 (1968)).

201. To make plain, when I am referring to queries that should be considered Fourth Amendment searches, I refer to them as query-searches.

202. *See supra* Part II.B.

203. *See generally* S. REP. NO. 95-701 (1978) (discussing the constraints on information use for collection methods); *see also* *Berger v. New York*, 388 U.S. 41 (1967) (stating that wiretapping must have limitations in order to adhere to the Fourth Amendment).

Nearly fifty years ago, concerns regarding the intrusive nature of wiretapping prompted the Supreme Court to augment the Fourth Amendment's typical warrant requirements (probable cause, particularity, and review by a neutral magistrate) with procedural rules about how the government handled the information it collected using that tool.²⁰⁴ The Supreme Court's ruling made it plain to Congress that, to satisfy constitutional demands, any use of wiretapping must include information handling limits.²⁰⁵ Thus when enacting legislative authorization for wiretapping, Congress included such limits, known collectively as minimization procedures.²⁰⁶ Minimization procedures regulate the government's handling of information so as to mitigate the risks that electronic surveillance poses for Americans' individual privacy rights.²⁰⁷ The statutes authorizing wiretapping for both domestic law enforcement and foreign intelligence purposes require minimization.²⁰⁸ While criminal investigations implement minimization requirements at the moment of collection,²⁰⁹ FISA requires minimization in the retention and dissemination of information as well in order to ensure "information concerning American citizens and lawful resident aliens be handled in such a way as to assure that it is used only for the purposes specified."²¹⁰ The constitutional need to minimize information has, over time, expanded beyond the wiretapping context and currently applies to collection of tan-

204. 388 U.S. 41 (1967).

205. *Id.*

206. See, e.g., *United States v. Duggan*, 743 F.2d 59, 73 (2d Cir. 1984) (citing S. REP. NO. 95-701, at 13 (1978)) ("FISA reflects both Congress's 'legislative judgment' that the court orders and other procedural safeguards laid out in [FISA] 'are necessary to insure that electronic surveillance . . . conforms to the fundamental principles of the fourth amendment [sic].'"); Berman, *supra* note 33, at 791-817 (discussing constitutional origins of minimization procedures); Donohue, *supra* note 72, at 220 ("FISA was Congress's express decision to curb executive power as a constitutional matter.").

207. 50 U.S.C. § 1801(h) (2012) (defining minimization procedures); PCLOB SECTION 702 REPORT, *supra* note 71, at 50 (asserting that minimization procedures impose a "set of controls on data" to "balance privacy and national security interests").

208. 18 U.S.C. § 2518(5) (every wiretap order "shall contain a provision that the authorization to intercept shall be . . . conducted in such a way as to minimize the interception of communications not otherwise subject to interception"); 50 U.S.C. §§ 1804, 1805 (requiring government surveillance applications and FISC authorization orders to include minimization procedures).

209. S. REP. NO. 95-701, at 41 (1978) (stating that criminal procedures are an exception to the minimization rule).

210. S. REP. NO. 95-604, at 38 (1977).

gible things, physical searches, and collection of communications metadata.²¹¹

The requirement to minimize is imposed statutorily; the task of determining exactly what minimization should look like in any particular circumstance, however, is left to the courts.²¹² Minimization procedures thus represent a mandate to courts to include limits on what the government may do with information gleaned from at least some forms of collection.

At times, courts have also imposed limits on the government's use of lawfully collected information even in the absence of a legislative requirement.²¹³ Recently, for example, the FISC considered whether the FBI's queries using U.S.-person selectors should be treated as searches subject to Fourth Amendment regulation.²¹⁴ While the court ultimately rejected the idea that such queries were themselves searches, it did not find them irrelevant to the constitutional analysis.²¹⁵ Instead, the use to which the government plans to put information collected under Section 702, the FISC concluded, should form part of the assessment of the reasonableness of the Section 702 program as a whole.²¹⁶ So while the FISC did not impose Fourth Amendment constraints directly on queries as such, it recognized the constitutional concerns that can arise out of some uses of information.²¹⁷

Postcollection use has also become an issue for computer searches. Because it is often not feasible to identify and isolate computer files responsive to a warrant at the time of seizure, it is common practice to make identical copies (or mirrors) of

211. See 50 U.S.C. § 1861(b)(2)(D) (collection of tangible things); *Id.* § 1881(a) (collection of electronic communications by targeting non-U.S. persons overseas); *Id.* § 1823(a) (physical searches for foreign intelligence purposes). Collection using a pen register or trap-and-trace device, which provides information about incoming or outgoing communications, now must employ "privacy procedures," which are simply minimization procedures by another name. *Id.* § 1842(h). See Berman, *supra* note 33, at 790–817. (providing a history of the evolution and development of minimization procedures).

212. Surveillance laws have consistently assigned the job of determining what minimization procedures are appropriate to the courts. 50 U.S.C. §§ 1805(a)(3), 1861a(1).

213. [Redacted] Memorandum and Opinion & Order at 41 (FISA Ct., Nov. 6, 2015); *id.* at 40 (rejecting the argument that "each query of Section 702–acquired information [using U.S.-person identifiers] is a 'separate action subject to the Fourth Amendment reasonableness test'").

214. *Id.*

215. *Id.* at 42.

216. *Id.* at 40–41.

217. *Id.* at 41–45.

computer hard drives to review their contents off-site.²¹⁸ In so doing, however, the government necessarily seizes a great deal of nonresponsive material—everything on the computer drive unrelated to criminal activity, such as family photos, contact lists, emails, and the like. Courts have recently grappled with how to limit the government’s access to or use of that nonresponsive information. In *United States v. Ganius*, for example, the court considered whether investigators can obtain a warrant to search a set of files the government happens to have in its possession because they were seized pursuant to a previous warrant, to which those files were not responsive.²¹⁹ A three-judge panel of the Second Circuit held that despite the valid initial collection of the information, the government violated the defendant’s Fourth Amendment rights by retaining the nonresponsive information in the absence of “some independent basis” for doing so.²²⁰ Permitting the government to “retain all the data on [an individual’s] computers on the off chance the information would become relevant to a subsequent criminal investigation,” the court said, would “be the equivalent of a general warrant.”²²¹ And in his concurring opinion in *In re Comprehensive Drug Testing*, Judge Alex Kozinski articulated a list of suggested guidelines for investigators to follow when executing searches that are likely to expose investigators to nonresponsive information.²²²

218. This two-step process of first seizing or copying digital storage devices and then searching its contents later is routine. See FED. R. CRIM. P. 41(e)(B).

219. 755 F.3d 125, 138 (2d Cir. 2014), *vacated on other grounds*, 824 F.3d 199 (2d Cir. 2016).

220. 755 F.3d at 138. The Second Circuit subsequently agreed to hear the case en banc, vacated the panel decision, and resolved the case on other grounds, declining to rule on the validity of the data retention or the second warrant. The en banc court did recognize, however, the highly intrusive nature of the government’s actions, observing that “the seizure of a computer hard drive, and its subsequent retention by the government, can give the government possession of a vast trove of personal information about the person to whom the drive belongs, much of which may be entirely irrelevant to the criminal investigation that led to the seizure.” *Id.*

221. *Id.* at 137; *accord* *United States v. Weikert*, 504 F.3d 1, 17 (1st Cir. 2007) (recognizing that “there may be a persuasive argument . . . that an individual retains an expectation of privacy in the future uses of her DNA profile”).

222. *United States v. Comprehensive Drug Testing, Inc.*, 621 F.3d 1162, 1178–80 (9th Cir. 2010) (en banc) (Kozinski, J., concurring). Some magistrate judges have also begun imposing limits on how the government executes searches of digital storage devices. See Orin S. Kerr, *Ex Ante Regulation of Computer Search and Seizure*, 96 VA. L. REV. 1241, 1246 (2010) (noting this

These isolated instances, while representing a tentative extension of Fourth Amendment rules into the use space in certain contexts, do not go far enough. Each of these examples represents what I call a collection-plus regime. Either Congress or the courts determine that collection rules alone are insufficient, so they augment those rules with use restrictions. Numerous commentators have also advocated some form of collection-plus regime, where postcollection use of information is considered relevant to the constitutionality of the original search or seizure.²²³ A collection-plus regime does not independently require use constraints, but instead applies them cumulatively, adding their procedural protections to those of the collection rules. The question is thus whether the whole of the government's action, from collection to use, complies with Fourth Amendment demands.

These collection-plus approaches take a step in the right direction by recognizing that the government's postcollection use, at least in certain circumstances, is constitutionally relevant. I contend, however, that collection-plus regimes do not go far enough. The most critical shortcoming of collection-plus is

practice and arguing that it is both unwise and beyond the scope of the magistrates' power).

223. See, e.g., Deven R. Desai, *Constitutional Limits on Surveillance: Associational Freedom in the Age of Data Hoarding*, 90 NOTRE DAME L. REV. 579, 625 (2014) (arguing for time limits on the use of data); Stephen E. Henderson, *Our Records Panopticon and the American Bar Association Standards for Criminal Justice*, 66 OKLA. L. REV. 699, 720 (2014) (advocating further development of use restrictions); Orin S. Kerr, *Executing Warrants for Digital Evidence: The Case for Use Restrictions on Nonresponsive Data*, 48 TEX. TECH L. REV. 1, 25 (2015) ("Although the seizure of nonresponsive files is reasonable when needed to effectuate the search for responsive files, subsequent use of the seized nonresponsive files transforms the nature of the seizure and renders it constitutionally unreasonable."); Harold J. Krent, *Of Diaries and Data Banks: Use Restrictions Under the Fourth Amendment*, 74 TEX. L. REV. 49, 51 (1995) (arguing that "the reasonableness of a seizure extends to the uses that law enforcement authorities make of property and information"); Robert S. Litt, *The Fourth Amendment in the Information Age*, 126 YALE L.J.F. 8, 15–16 (2016) (arguing that courts assessing the constitutionality of government action should take into account "not only the nature of the data the government is collecting, but the use the government is going to make of that data"); Peter Swire, *A Reasonableness Approach to Searches After the Jones GPS Tracking Case*, STAN L. REV. ONLINE, Feb. 2012, <https://www.stanfordlawreview.org/online/privacy-paradox-a-reasonableness-approach-to-searches-after-the-jones-gps-tracking-case> (arguing that factors such as the length and intrusiveness of surveillance as well as the use of minimization procedures, if any, should factor into the question whether the government search was reasonable); cf. Jennifer Daskal, *The Un-Territoriality of Data*, 125 YALE L.J. 326, 388 (2015) (noting that acquisition and use restrictions "must go hand-in-hand").

that when it comes to Fourth Amendment-exempt information—such as third-party records—there is no constitutional analysis into which one could incorporate limits on the government's postcollection use.²²⁴ For all the vast spectrum of information, ranging from the innocuous to the intensely private, that is exempt from Fourth Amendment coverage, courts have no opportunity to consider whether the use of that information renders its collection unreasonable, because the Fourth Amendment's reasonableness requirement does not apply in the first place.²²⁵ Moreover, it is not clear at the time of collection whether or when the aggregation problem will arise with respect to particular data. The insight that aggregation permits may result only from the combination of data sets that are fused after—perhaps years after—the collection has taken place.²²⁶ The idea of assessing the government's action as a whole in those circumstances is unwieldy at best. If you accept the argument that queries of aggregated information reveal more than the individual bits of information the government collects, we must recognize those uses themselves as searches entitled to their own independent Fourth Amendment analysis, regardless of how the underlying information was collected.

2. Implementing Query-Search Limits

If one accepts the argument that courts should assess query-searches independently of the means by which the information was collected, the question becomes how they might do so. Here, I argue that the FISC has already shown us what such an analysis might look like. Indeed, the minimization procedures that FISC judges demanded in their orders approving

224. Donohue, *supra* note 72, at 243 (describing Professor Kerr's argument that "because third-party record collection constitutes neither a search nor a seizure, the doctrine would have to be radically overhauled to make all collection of data a seizure to then trigger a reasonableness analysis").

225. *United States v. Knotts*, 460 U.S. 276 (1983) (holding that it is neither a search nor a seizure to monitor the location of a beeper placed in chemicals being transported to owner's cabin); *Smith v. Maryland*, 442 U.S. 735 (1979) (holding that a telephone company's use of a pen register is not a search); *Hofa v. United States*, 385 U.S. 293 (1966) (holding that testimony from conversations between government informant and defendant did not violate the search and seizure limits of the Fourth Amendment). *But see United States v. Karo*, 468 U.S. 705 (1984) (holding it is a search to monitor a beeper that is inside a house and therefore withdrawn from public view).

226. *See* PCAST, *supra* note 54 at ix; *id.* at xii (noting that collection rules cannot guard against future, unknown privacy threats, so use is "the technically most feasible place to protect privacy").

the Section 215 bulk metadata collection program look more like the Fourth Amendment warrant requirement procedures than anything else.²²⁷ The Section 215 program itself was not subject to Fourth Amendment limits because the government argued, and the FISC agreed, that the metadata collection fell within the scope of the third-party doctrine.²²⁸ The statutes required minimization procedures, but given the absence of Fourth Amendment demands, such procedures could have been nominal. As I have argued elsewhere, in imposing robust limits on query-searches of the Section 215 database nonetheless, the FISC signaled recognition of those query-searches' Fourth Amendment-based implications and demonstrated how other, similarly intrusive query-searches might be subject to Fourth Amendment oversight.²²⁹

Before demonstrating this point, a quick primer on the purposes of each of the warrant requirement's three elements is in order. First, there is *ex ante* review by a neutral magistrate, based on the idea that officials with "investigative and prosecutorial duty should not be the sole judges of when to utilize constitutionally sensitive means The historical judgment, which the Fourth Amendment accepts, is that unreviewed executive discretion may yield too readily to pressures to obtain" information and "overlook potential invasions of privacy and protected speech."²³⁰ Second, the cause requirement limits arbitrary government action.²³¹ In forcing the government to demonstrate that there is an answer to the question why are you searching this person or seizing this information?, cause requirements guarantee that the search or seizure will be based on objective evidence, rather than the exercise of unfet-

227. See *infra* notes 234–39 and accompanying text. For a detailed discussion of the Section 215 use regime and its constitutional shadings, see Berman, *supra* note 33, at 806–17.

228. See *In re* [REDACTED], No. PT/TT [REDACTED] (FISA Ct., July 14, 2004). The limits on the collection of that data were statutory: the information had to be both "relevant" to an authorized terrorism or intelligence investigation and subject to minimization procedures. Foreign Intelligence Surveillance Act, 50 U.S.C. § 1861(b) (2015).

229. See Berman, *supra* note 33, at 817–24.

230. *United States v. U.S. Dist. Court (Keith)*, 407 U.S. 297, 317 (1972).

231. See Barry Friedman & Cynthia Benin Stein, *Redefining What's "Reasonable": The Protections for Policing*, 84 GEO. WASH. L. REV. 281, 317 (2016) ("[T]he sine qua non of official arbitrariness is allowing officers unfettered 'discretion' to search whenever the whim strikes."). Individualized suspicion requirements reduce the likelihood of government intrusion on the basis of (implicit or explicit) bias, individual animus, or other improper motives. *Id.* at 317–20.

tered executive discretion.²³² Third, the particularity requirement prevents the government from “rummag[ing] through homes in an unrestrained search for evidence of criminal activity.”²³³ So just as the government must explain why it has singled out a particular individual, it must also explain exactly what it expects the search to yield. Together, these requirements ensure that a government determination to intrude into an individual’s private realm is both objectively justified and limited in scope.

The FISC imposed approximations for each of these elements in its oversight of the Section 215 program. First, it required all queries to be approved through *ex ante* review by a high-ranking government official. If the query-search involved “seed accounts . . . used by U.S. persons,” approval had to come from the NSA’s Office of General Counsel (NSA OGC).²³⁴ So while individual determinations regarding whose metadata would be accessed did not require *judicial* preapproval, the NSA OGC’s approval did serve to diminish discretion by ensuring that officers with “investigative and prosecutorial duty” were not “the sole judges” of when to execute queries about U.S. persons.²³⁵ While someone in the NSA’s OGC is not an independent magistrate, she is more able to make an impartial assessment than an agent or official actually involved in an investigation.

Second, the FISC imposed a cause standard on Section 215 query-searches, in the form of the “reasonable articulable sus-

232. When the courts have not insisted on individualized suspicion, they have usually insisted on some other means of limiting the discretion of the officers in the field. *See* *Delaware v. Prouse*, 440 U.S. 648, 654–55 (1979) (holding that when the circumstances preclude “insistence upon ‘some quantum of individualized suspicion,’ other safeguards are generally relied upon to assure that the individual’s reasonable expectation of privacy is not ‘subject to the discretion of the official in the field’” (quoting *Camara v. Mun. Court*, 387 U.S. 523, 532 (1967))); *Friedman & Stein*, *supra* note 231, at 310 (quoting *Brown v. Texas*, 443 U.S. 47, 52–53 (1979)). *But see* Eve Brensike Primus, *Disentangling Administrative Searches*, 111 COLUM. L. REV. 254, 278–79 (2011) (arguing that the special needs doctrine permits suspicionless searches with no limits on discretion).

233. *Riley v. California*, 134 S. Ct. 2473, 2494 (2014) (citations omitted) (pointing out that “the Fourth Amendment was the founding generation’s response to the reviled ‘general warrants’ . . . of the colonial era,” which permitted indiscriminate searches).

234. *In re Application of the FBI for an Order Requiring the Prod. of Tangible Things from [REDACTED]*, No. BR 06-08, 6 (FISA Ct., Aug. 18, 2006).

235. *Id.*

picion” requirement.²³⁶ This standard required a determination that, “based on the factual and practical considerations of everyday life on which reasonable and prudent persons act, there are facts giving rise to a reasonable articulable suspicion (RAS) that [the particular seed] to be queried is associated with [REDACTED—probably ‘an international terrorist organization’ or ‘Al Qaeda’].”²³⁷ The FISC actually saw the reasonable articulable suspicion standard as analogous to a cause requirement, asserting that imposing this limit on query-searches would ensure “that [t]he information actually viewed by any human being . . . will be just as limited—and will be based on the same targeted, individual standards” as searches governed by the Fourth Amendment.²³⁸

Finally, the reasonable articulable suspicion standard steps in for the particularity requirement as well. That collection of everyone’s telephone metadata will net a huge amount of irrelevant information is a certainty.²³⁹ Because query-searches could be directed only at those seed identifiers for which the government had reasonable articulable suspicion of connection to a terrorist organization, however, the government is limited to inquiries that will yield information related to the communications of suspected terrorists and their associates. Government officials could not query the database in search of nonterrorism-related crimes or threats.

These minimization requirements are not identical to the ones that would apply to the collection of information whose seizure required a warrant. But they do create proxies for each of those traditional protections. The FISC thus employed minimization rules to impose limitations that clearly took Fourth Amendment concerns into account.

3. Implications for Surveillance Programs and Beyond

Query-searches could be subjected to a regime similar to the one the FISC imposed on the Section 215 program.²⁴⁰ This

236. *In re* Application of the FBI for an Order Requiring the Prod. of Tangible Things from [REDACTED], No. BR 13-80, 3 (FISA Ct., Apr. 25, 2013).

237. *Id.* No U.S.-person seed could meet the RAS standard solely on the basis of activities protected by the First Amendment. *Id.*

238. *In re* [REDACTED], No. PR/TT [REDACTED], 58 n.41 (FISA Ct., July 14, 2004) (internal quotations and emphasis omitted).

239. *In re* Application of the FBI for an Order Requiring the Prod. of Tangible Things from [REDACTED], No. BR 13-109, 18 (FISA Ct., Aug. 29, 2013).

240. This Article does not advocate interpreting the Fourth Amendment to require for all query-searches the exact same rules that the FISC imposed in

is perhaps most compelling in the context of querying Americans' Section 702-acquired communications, which includes the contents of U.S. persons' communications with overseas targets. The government takes advantage of the absence of constitutional limits to query-search Section 702-acquired information using selectors associated with U.S. persons, thereby gaining access to the contents of Americans' communications with no individualized suspicion, no particularity requirement, and no *ex ante* review. Hence the "backdoor loophole" moniker by which such query-searches are known.

Unfortunately, the FISC rejected the argument that these queries should be treated as searches, instead holding that they should be subject to a collection-plus regime.²⁴¹ According to the FISC opinion, the queries are not themselves searches, but their use must be factored in to the constitutionality of the Section 702 program as a whole.²⁴² But the constitutionality of the government's access to U.S. persons' communications content should not be dependent on how other aspects of the Section 702 program operate. Access to Americans' communications content is at the heart of traditional Fourth Amendment protection. The same rules should apply whether the government accesses that information from a database sitting on its own servers, secures a warrant to acquire that information from a communications provider's server, or executes a warrant to seize an individual's personal computer. Section 702 query-searches should be considered reasonable only when the government can demonstrate to an executive branch official, or (even better) to the FISC itself, individualized suspicion about the target of the query-search.²⁴³ Moreover, a particularity requirement should limit the government to query-searches that are designed to return information relevant to the purpose of the program—foreign intelligence information. This would allow the government to both continue employing Section 702 for its original purpose—the collection of foreign intelligence—and prevent the use of U.S.-person identifiers to access communica-

the Section 215 program. Once queries are recognized as searches, reasonable minds can disagree regarding what those rules should be; I defer to another day the difficult task of answering that question.

241. See *supra* notes 216–17 and accompanying text.

242. *Id.*

243. The USA FREEDOM Act of 2015 requires the government to seek FISC approval for any queries of telephone metadata. USA FREEDOM Act of 2015, Pub. L. No. 114-23, § 101, 129 Stat. 268 (2015) (codified at 50 U.S.C. § 1861 (2012)).

tions to which it would not have lawful access in the absence of Section 702.

Query-searches are not limited to the foreign intelligence context. Government officials of all types utilize databases to seek out information about U.S. persons. In fact, before even opening an official investigation, FBI agents are authorized to examine not only all FBI and Department of Justice records, but also “records maintained by . . . other federal, state, local, or tribal, or foreign governmental entities or agencies.”²⁴⁴ Such inquiries require an “authorized purpose,” but no individualized suspicion.²⁴⁵ This authority may be used to obtain information “on individuals, groups, or organizations of possible investigative interest,” either because they may be involved in crime or threats to the national security “or because they may be targeted for attack or victimization.”²⁴⁶ Thus federal agents have a green light to query any and all databases available to them about U.S. persons even in the absence of individualized suspicion.

Queries of government databases by federal, state, local, or tribal law enforcement entities can prove just as intrusive as those used in the Section 215 or Section 702 programs. The NYPD’s DAS, for example, can track where a particular car is located and where it has been the past days, weeks, or months and it can aggregate that information with license plate information, as well as watch lists and criminal history.²⁴⁷ In other words, it allows the police to identify connections between persons, places, and things in ways that a human crime analyst may not have been able to do.²⁴⁸ Cross-referencing the federal government’s biometric databases with surveillance camera footage or photos on social media websites could provide an hour-by-hour account of a particular individual’s location and activities.²⁴⁹ Imagine a query compiling financial records with information about products with RFIDs. Such a query would

244. FED. BUREAU INVESTIGATIONS, THE ATTORNEY GEN.’S GUIDELINES FOR DOMESTIC FBI OPERATIONS 20 (2008).

245. Authorized purposes are “to detect, obtain information about, or prevent or protect against federal crimes or threats to the national security or to collect foreign intelligence.” *Id.* at 19.

246. *Id.* at 17.

247. *See* Joh, *supra* note 11, at 48–49.

248. *Id.*

249. *See* Jennifer Lynch, *FBI’s Facial Recognition Is Coming to a State Near You*, ELECTRONIC FRONTIER FOUND. (Aug. 2, 2012), <https://www.eff.org/deeplinks/2012/07/fbis-facial-recognition-coming-state-near-you>.

indicate what one purchases and where (or to whom) it goes. Similarly, combining employment records with travel records could expose the fact that your last sick day was actually a three-day weekend at the beach.

Sometimes database queries will be highly effective tools used to locate criminals, and this Article does not argue that the government should be barred from using them wholesale. Instead, the argument is merely that when the government uses a U.S.-person identifier to search aggregated information, that query should often qualify as a search and the Constitution should impose limits on those queries, just as it does a search of your home or a stop-and-frisk on the street.

C. THE INDISPENSABILITY OF CONSTITUTIONAL REGULATION

The foregoing discussion has largely focused on what the *Constitution* requires or permits. But, of course, the Constitution is not the only means of regulating government conduct. Many of the government's collection techniques (as well as some uses) are subject to statutory, regulatory, or policy-based limits. Here, I explain why these existing nonconstitutional rules do not sufficiently address the concerns raised by query-searches, and will not likely do so in the future.

Those who are content to rely on legislative or regulatory action to impose limits on the government's use of new technologies argue that policy makers are better suited than courts to determine appropriate constraints.²⁵⁰ Congress's past performance in regulating to protect privacy, however, does not support this approach. Legislative measures addressing perceived shortcomings in data privacy are almost universally perceived as outdated, incomplete, insufficiently rigorous, or some combination of the three.²⁵¹ The United States lacks an overarching,

250. *E.g.*, Kerr, *supra* note 121, at 857–81 (arguing that courts do not respond to new technological challenges swiftly enough and that we should rely on the legislature to do so instead); Peter Margulies, *Searching for Judicial Power: Article III and the Foreign Intelligence Surveillance Court* (Roger Williams Univ. Sch. of Law, Working Paper No. 171, 2016), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2827767 (arguing that Congress should be given deference in making decisions related to national security and evolving technology). *But see, e.g.*, Swire, *supra* note 81, at 915–19 (expressing skepticism regarding Congress's ability to protect privacy effectively).

251. *See, e.g.*, Solove, *Access and Aggregation*, *supra* note 36, at 1154 (“Our information regulatory infrastructure is disconnected, often outdated, and inadequate to meet the challenges of the new technologies of the Information Age.”). ECPA requires a warrant for collecting the contents of your e-mail, but

unified information protection regime. Instead, when Congress has acted at all, it has done so piecemeal, through a series of narrowly targeted statutes.²⁵²

The USA Freedom Act of 2015 might initially paint a promising picture.²⁵³ After all, the FISC did impose Fourth Amendment–like minimization procedures on the Section 215 program,²⁵⁴ the reauthorization debate as the statute approached its sunset date was intense, and Congress ended up codifying, in large part, the FISC’s judicially imposed limits on Section 215’s scope.²⁵⁵ Indeed, one provision in the legislation

not for collecting other data stored in the cloud. *See, e.g.*, Kerr, *supra* note 90, at 1213–18.

252. *See* Daniel J. Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy*, 53 STAN. L. REV. 1393, 1430–45 (2001) [hereinafter Solove, *Privacy and Power*] (discussing the “limits of privacy law” and identifying flaws in multiple privacy statutes, including those protecting information about credit records, health, and education, as well as information included on drivers’ licenses and in electronic communications); Taipale, *supra* note 58, at 53–55 n.223 (comparing the piecemeal U.S. information privacy regime with Europe’s more comprehensive approach); Solove, *Privacy and Power*, *supra*, at 1440 (“Since the 1970s, Congress has grappled with the problem of databases, but has been slow to take action.”). Moreover, when statutory protections do apply, those “protections” are much less rigorous than typical Fourth Amendment rules, often dispensing with *ex ante* review or individualized suspicion. Solove, *Privacy and Power*, *supra*, at 1430–45. Statutory limits often set a low threshold for the government to meet. *E.g.*, Stored Communications Act, 18 U.S.C. § 2703(d) (2012) (information must be “relevant and material to an ongoing . . . investigation”); *Id.* § 2703(d) (requiring “specific and articulable facts” (but not probable cause) giving reasonable grounds to believe the information will be relevant and material to an ongoing investigation). Most information in the hands of third parties may be acquired simply by issuing a subpoena, some of which may be issued by prosecutors or law enforcement officials with no prior judicial approval. *E.g.*, *id.* § 3486 (administrative subpoenas); *id.* § 2709 (national security letters, which permit the FBI to get customer’s telephone toll and transactional records); *see also* 12 U.S.C. § 3414; 15 U.S.C. § 1681u (banking, financial, and credit information).

253. USA FREEDOM Act of 2015, Pub. L. No. 114-23, 129 Stat. 268 (codified at 50 U.S.C. § 1861) (barring bulk collection of telephone and Internet metadata). As I have argued elsewhere, the USA FREEDOM Act was a shift in the right direction, but it did not do nearly enough. *See* Emily Berman, *The Two Faces of the Foreign Intelligence Surveillance Court*, 91 IND. L.J. 1191 (2016).

254. *See supra* notes 234–39 and accompanying text.

255. In modifying the Section 215 authorities in the USA FREEDOM Act of 2015, Congress retained many of the limits initially imposed as minimization procedures by the FISC. The legislation preserved the individualized cause requirement by codifying the RAS standard. 50 U.S.C. § 1861(b)(2)(C) (to access calling records the government must show “there is a reasonable, articulable suspicion” that the seed identifier—the “special selection term” (SST) in the language of the statute—“is associated with” a foreign power or an agent of a foreign power “engaged in international terrorism”). The statute also in-

was even more restrictive than the one the FISC required, perhaps because some legislators argued the Constitution demanded it.²⁵⁶ Thus we had a regulatory regime that was adopted, refined in part due to constitutional concerns, and codified by Congress. Problem solved, right? Wrong.

To the extent the USA Freedom Act is a success story, it is the exception, not the rule. As an initial matter, the prior version of Section 215 had a sunset date. And while sunsets alone are not usually sufficient to force policy changes, this sunset provision followed closely on the heels of Edward Snowden's massive leak of information about U.S. surveillance activities.²⁵⁷ That leak revealed that the government was interpreting Section 215 of FISA in an expansive and highly controversial way. In other words, the revelation of a secret program, targeted at Americans, and interpreting executive collection powers in the most aggressive way possible was enough to prompt Congress to restrict query-searches in that context. By contrast, Section 702 sunsets on December 31, 2017, yet there has been no public outcry objecting to the way the government query-searches the communications of Americans scooped up that program. Some legislators believe that such query-searches violate the Fourth Amendment, but that view has not led to change, nor does it seem likely that it will.²⁵⁸

cluded a particularity requirement. *Id.* §§ 1861(k)(4)(B), 1861(c)(2)(A) (allowing collection regarding only an SST that "specifically identifies an individual, account, or personal device" and requiring that the FISC's order describe "each specific selection term . . . with sufficient particularity to permit them to be fairly identified"). The statute's *ex ante* review requirement differed from the FISC's Section 215 minimization rules in that it requires prior review by the FISC itself rather than internal executive branch officials. *Id.* § 1861(a).

256. *E.g.*, 161 CONG. REC. H2916 (daily ed. May 13, 2015) (statement of Rep. Nadler) ("[T]he dragnet collection without a warrant of telephone records . . . is the contemporary equivalent of the British writs of assistance . . . that the Fourth Amendment was drafted to outlaw."); 161 CONG. REC. H2920 (daily ed. May 13, 2015) (statement of Rep. Jeffries) ("[E]nding bulk collection through section 215" was a step toward "restoring the balance" between effective national security and respect for privacy demanded by the Constitution).

257. See Emily Berman, *The Paradox of Counterterrorism Sunset Provisions*, 81 FORDHAM L. REV. 1777 (2013) (arguing that sunsets fail to prompt legislative reform unless they coincide with a scandal of some kind).

258. *E.g.*, 161 CONG. REC. E726-04 (2015) (statement of Rep. Sensenbrenner) ("Section 702 of FISA has been improperly used to obtain the content of Americans' private communications without a warrant, which is unconstitutional under the Fourth Amendment."); 161 CONG. REC. H2923 (daily ed. May 13, 2015) (statement of Rep. Sanford) ("The notion that Americans' rights are contingent on the geography of where a call is directed is not consistent with the Constitution and highlights why [Section 702] needs to be changed.").

The perfect storm that swept the USA Freedom Act into existence is not something we can count on happening regularly. The Snowden leaks are likely a once-in-a-generation event. The only comparable historical event is the leak of the Pentagon Papers half a century ago. The Snowden leaks not only triggered sufficient outrage regarding Section 215 to motivate legislative action; they also brought to light the very existence of the program. If Congress or the American public are not aware of the way the government is using information, legislative action is impossible. Thus the FBI's efforts to keep its use of Stingrays under wraps ensured that the public lacked sufficient information to generate or enable opposition by legislators or their constituents. Nor do most people know whether and how their state or local law enforcement agencies employ information gathered from Stingrays, license plate readers, surveillance camera footage, or other modern collection methods.

Congress's efforts to fill perceived statutory holes in the privacy regime, when they do come, have sometimes stalled indefinitely. For years, there has been bipartisan consensus, for example, that the Electronic Communications Privacy Act needs to be updated to reflect current technology.²⁵⁹ The Email Privacy Act, a reform bill, passed the House of Representatives 419–0.²⁶⁰ Yet it still languishes, caught up in debate over when the government will be able to access information protected by the law.²⁶¹

Reliance on regulatory regimes imposed on query-searches through minimization requirements warrants similar skepticism. First, foreign intelligence collection is effectively the sole context to which minimization requirements apply. Among all of the domestic law enforcement tools, only the law regulating wiretaps requires the government to minimize. And there, minimization applies only to the collection stage, rather than the retention, use, and dissemination stages that dominate FISA

259. James Stiven, *ECPA Reform Will Protect Privacy and Meet Law Enforcement Needs*, HILL (June 2, 2016), <https://www.thehill.com/blogs/pundits-blog/technology/281987-ecpa-reform-will-protect-privacy-meet-law-enforcement-needs> (noting that “[f]ew problems in recent years have drawn more extensive bipartisan support” than ECPA reform).

260. Email Privacy Act, H.R. 699, 114th Cong. (2015); H.R. REP. NO. 114-528 (2015).

261. Marcy Wheeler, *Why Is the Government Poison-Pilling ECPA Reform?*, EMPTYWHEEL (June 7, 2016), <https://www.emptywheel.net/2016/06/07/why-is-the-government-poison-pilling-ecpa-reform>.

minimization.²⁶² Moreover, minimization in the criminal context sometimes seems to be more honored in the breach, thanks in part to the Supreme Court's reluctance to suppress evidence based on failure to minimize.²⁶³ If the Fourth Amendment applied to all query-searches, courts would be required to impose necessary constraints in all areas of law, not just in wiretaps and foreign intelligence surveillance.

Second, minimization procedures apply only to information not available publicly. Depending on how broadly the concept of public information is construed, this could include a great deal of the information that the government collects under Fourth Amendment exemptions or purchases from third parties. Yet, as *U.S. Department of Justice v. Reporters Committee for Freedom of the Press* recognized, the aggregation of publicly available information can be quite revealing.²⁶⁴

Third, one common means of minimizing data is to strip out any personally identifying information.²⁶⁵ As more and more information becomes available, however, rediscovering the personally identifiable information, even after it has been stripped is relatively easy to do. Some attributes are uniquely identifying on their own, but more importantly any attribute can be identifying in combination with others. One study showed that by combining "public, Personal Genome Project profiles containing zip code, birthdate, and gender with public

262. See Berman, *supra* note 33, at 790–99.

263. See *Scott v. United States*, 436 U.S. 128, 139–42 (1978) (holding that the failure of agents executing a wiretap warrant to make a good faith effort to minimize interception did not require suppression); James X. Dempsey, *Communications Privacy in the Digital Age: Revitalizing the Federal Wiretap Law To Enhance Privacy*, 8 ALB. L.J. SCI. & TECH. 65, 77 (1997) ("The minimization requirement . . . has not been strictly enforced . . ."); Peter J. Georgiton, *The FBI's Carnivore: How Federal Agents May Be Viewing Your Personal E-mail and Why There Is Nothing You Can Do About It*, 62 OHIO ST. L.J. 1831, 1860 (2001) ("The [Scott] Court's determination of what factors constitute 'reasonableness' for the purposes of minimization requirements has been applied by lower courts to justify a variety of broad searches.").

264. See *U.S. Dep't of Justice v. Reporters Comm. for Freedom of Press*, 489 U.S. 749, 763–64 (1989).

265. Personally identifiable information is

information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.

Memorandum from Clay Johnson III, Deputy Dir. for Mgmt., U.S. Office of Mgmt. & Budget to the Heads of Exec. Dep'ts & Agencies, M-07-16 n.1 (May 22, 2007).

voter rolls, and mining for names hidden in attached documents, 84–97 percent of the profiles” could be accurately matched with a name.²⁶⁶ As technology advances, minimization practices like anonymization and data deletion that have been used for privacy protection in the past are not going to work because they are “increasingly easily defeated by the very techniques” that are used in analyzing data.²⁶⁷

Finally, another crucial difference between constitutional doctrine and the implementation of statutes and regulations is their transparency. Another lesson Edward Snowden taught us is that knowing the language of the statute is not always sufficient to understand exactly how that statute is being implemented. Rules that impact fundamental rights like privacy should be entirely public.²⁶⁸ Too often, agency interpretations, guidelines, targeting and minimization procedures, and other limits originating in the executive branch have remained secret. This is not the case when it comes to judicial opinions, and to the extent the rules are developed by the FISC (whose decisions often are classified), any statutory or constitutional interpretation that court engages in also must be made public.

Since neither statutory nor minimization-based constraints will successfully alleviate concerns regarding the intrusiveness of query-searches, Constitution-based rules must be developed. To be sure, such rules will impose costs and burdens on government agencies and officials, potentially reducing investigative efficiency. On the other hand, forcing government officials to target only those individuals for whom individualized suspicion exists could improve efficiency, eliminating fruitless fishing expeditions. More importantly, however, not all limits on government activity are designed to maximize efficiency. Rather, some are there to protect individual rights, even if such protection renders governance incrementally less efficacious.

CONCLUSION

Throughout the nation’s history, changes in the technology to which the government has access when conducting investigations have prompted adjustments in legal doctrine. Today as

266. PCAST, *supra* note 54, 39–40.

267. *Id.* at xi, 38.

268. See generally Dakota S. Rudesill, *Coming to Terms with Secret Law*, 7 HARV. NAT’L SEC. J. 241 (2015) (arguing against the idea of secret law and in favor of a presumption that the rules available to the public accurately inform the polity of what the government is doing).

never before, technology has steamed ahead at a pace with which the law has struggled (unsuccessfully) to keep up. Today's technology provides not only better versions of existing tools; it also provides entirely new tools, tools that do not fit neatly into any of our doctrinal paradigms. The government has gone from building profiles on individuals by seeking out paper files from disparate sources in various jurisdictions to aggregating massive amounts of data with the click of a mouse. This capacity to aggregate information, when combined with the amount of detailed information about each of our lives that is digitally captured and preserved, is not just a better mouse-trap; it is a global mouse vaporizer. That is to say, it must be recognized as a new phenomenon, not merely a more effective version of an existing tool. While the phenomenon is new, the red flags it raises are as old as government itself. Fortunately, our founding document speaks not in the language of technology but in the language of rights. And those rights must be preserved even in the face of an information revolution in a digital age. When queries of aggregated information reveals knowledge in which U.S. persons have a reasonable expectation of privacy, the Fourth Amendment right to be secure in our persons, houses, papers, and effects is triggered just as surely as if the government had entered our home and physically sorted through our financial, medical, familial, and associational records. Such queries therefore demand the same label as such a home invasion: search.

THE MANY REVOLUTIONS OF *CARPENTER*

*Paul Ohm**

TABLE OF CONTENTS

I. INTRODUCTION.....	358
II. THE NEW RULE OF <i>CARPENTER</i>	361
<i>A. Carpenter's Broad New Rule</i>	361
<i>B. On Police Efficiency and Time Machines</i>	366
<i>C. What is the Carpenter Test?</i>	369
1. First Factor: Deeply Revealing Nature.....	371
2. Second Factor: Depth, Breadth, and Comprehensive Reach.....	372
3. Third Factor: The Inescapable and Automatic Nature of the Collection.....	376
4. The Test.....	378
<i>D. Applying the Carpenter Test</i>	378
1. Very Likely Covered: Web Browsing Records.....	378
2. Most Likely Covered: Massive Collections of Telephone and Bank Records.....	381
3. Uncertain Application: Databases of Medical Records and Genetic Information	383
III. BEYOND THE CORE TEST OF <i>CARPENTER</i>	385
<i>A. Carpenter as a Replacement for Katz</i>	385
1. The Subjective Prong: <i>Katz</i> Has Only One Step	386
2. The Objective Prong: Victory of the Normative Fourth Amendment.....	387
3. The Argument for Moving Beyond <i>Katz</i>	389
<i>B. The Third-Party Doctrine, Inside Out</i>	390
<i>C. Carpenter and Direct Government Surveillance</i>	392
<i>D. The New Rule of Technological Equivalence</i>	394
1. Information from Inside the Home.....	394
2. Bailment	396
3. Private Communications	398
IV. <i>CARPENTER'S</i> TECH EXCEPTIONALISM	399
<i>A. Rejecting Conventional Analogies</i>	400

* Professor of Law and Associate Dean, Georgetown University Law Center. Thanks for excellent comments to the faculty of the University of Baltimore School of Law and the students of the law schools at Fordham and the University of Texas. Special thanks to Lindsey Barrett, Alvaro Bedoya, Steve Bellovin, Oren Bracha, Bobby Chesney, Danielle Citron, Julie Cohen, Andrew Ferguson, John Golden, Orin Kerr, Marty Lederman, and Laura Moy for comments. Thanks also to Mario Trujillo for research assistance.

<i>B. The Chief Justice's Tech Exceptionalism</i>	401
<i>C. The Argument for Tech Exceptionalism</i>	403
<i>D. Expertise and Analogy</i>	405
<i>E. Time and Technological Change</i>	408
<i>F. Refusing to Look Backwards</i>	410
1. The Surveyors	410
2. The Legal Historians	412
3. The Positive Law Proponents	413
4. Looking Forward Not Backward	413
V. CONCLUSION	415

I. INTRODUCTION

The Supreme Court's opinion in *Carpenter v. United States*¹ has been heralded by many as a milestone for the protection of privacy in an age of rapidly changing technology.² Despite this, scholars and commentators have failed to appreciate many of the important aspects of this landmark opinion. *Carpenter* works a series of revolutions in Fourth Amendment law, which are likely to guide the evolution of constitutional privacy in this country for a generation or more.

The most obvious revolution is the case's basic holding — information about the location of cell phone customers held by cell phone providers is now protected by the Fourth Amendment, at least when the police seek seven days or more of such information.³ For the first time, the Court has held that the police must secure a warrant to require a business to divulge information about its customers compiled for the business's purposes, reinventing the reasonable expectation of privacy test and significantly narrowing what is known as the third-party doctrine.⁴ This cell-site location information (“CSLI”) has become a key

1. 138 S. Ct. 2206 (2018).

2. See, e.g., Daniel Solove, *Carpenter v. United States, Cell Phone Location Records, and the Third Party Doctrine*, TEACHPRIVACY (July 1, 2018), <https://teachprivacy.com/carpenter-v-united-states-cell-phone-location-records-and-the-third-party-doctrine> [https://perma.cc/M9GD-CD6Q]; Lior Strahilevitz & Matthew Tokson, *Ten Thoughts on Today's Blockbuster Fourth Amendment Decision — Carpenter v. United States*, CONCURRING OPINIONS (June 22, 2018), <https://concurringopinions.com/archives/2018/06/ten-thoughts-on-todays-blockbuster-fourth-amendment-decision-carpenter-v-united-states.html> [https://perma.cc/Y94X-PTXR] [hereinafter Strahilevitz & Tokson, *Ten Thoughts*]; Orin Kerr, *First Thoughts on Carpenter v. United States*, REASON: THE VOLOKH CONSPIRACY (June 22, 2018, 12:20 PM), <https://reason.com/volokh/2018/06/22/first-thoughts-on-carpenter-v-united-sta> [https://perma.cc/MM3L-928T].

3. *Carpenter*, 138 S. Ct. at 2217, 2217 n.3 (“It is sufficient for our purposes today to hold that accessing seven days of [cell-site location information] constitutes a Fourth Amendment search.”).

4. *Id.* at 2221.

source of evidence for criminal investigations, so this holding will revolutionize the way the police build their cases, requiring a warrant where none has been required before.⁵

Building outward, the reasoning of the majority opinion, written by Chief Justice Roberts and commanding five votes, revolutionizes the law of police access to many other types of information, in addition to CSLI.⁶ Databases that can be used, directly or indirectly, to ascertain the precise location of individuals over time are likely now covered by the Fourth Amendment. The police will probably need a warrant to obtain location information collected by mobile apps, fitness trackers, connected cars, and many so-called “quantified self” technologies.⁷

The reasoning extends beyond location information, although predicting the scope and shape of this revolutionary step requires a bit more speculation. The majority opinion promulgates a new, multi-factor test that will likely cover other commercially significant data that the police have begun to access in its investigations.⁸ Massive databases of web browsing habits stored by internet service providers (ISPs)⁹ will probably now require a warrant to access. Perhaps most surprisingly, the majority’s reasoning will apply even to massive databases of telephone dialing and banking records, cutting back on the holdings of two cases, *Smith v. Maryland*¹⁰ and *Miller v. United States*,¹¹ that the *Carpenter* Court expressly declined to overrule.¹² Those two cases are in a much more precarious state than other commenters have recognized.¹³

Looking beyond the central holding and reasoning, to dicta from the majority and dissenting opinions, another class of revolutions comes into view. The Court has breathed new life into *Kyllo v. United States*,¹⁴ the 2001 case that required the police to obtain a warrant to aim a thermal imaging device at a private home.¹⁵ At least seven justices of the *Carpenter* Court suggest a heretofore unrecognized rule

5. *Id.* at 2233 (Kennedy, J., dissenting) (“[T]he Court’s holding . . . limits the effectiveness of an important investigative tool for solving serious crimes.”)

6. *See infra* Section III.D.

7. Andrew G. Ferguson, *The Smart Fourth Amendment*, 102 CORNELL L. REV. 547, 591–95 (2017) (discussing Fourth Amendment implications of GPS monitors attached to the body). For a discussion of these technologies, *see infra* note 51.

8. *See infra* Section II.D.

9. *See generally* Paul Ohm, *The Rise and Fall of Invasive ISP Surveillance*, 2009 U. ILL. L. REV. 1417, 1438–40 (2009), [hereinafter Ohm, *Invasive ISP Surveillance*] (describing the power of ISPs to scrutinize the private browsing habits of customers).

10. 442 U.S. 735 (1979).

11. 425 U.S. 435 (1976).

12. *Carpenter v. United States*, 138 S. Ct. 2206, 2220 (2018) (“We do not disturb the application of *Smith* and *Miller* . . .”).

13. *See, e.g.*, Solove, *supra* note 2 (“The Supreme Court should have overruled the Third Party Doctrine or at least carved out a greater chunk of it.”).

14. 533 U.S. 27 (2001).

15. *Id.* at 40.

building on *Kyllo*: the *rule of technological equivalence*. If a technology, or a near-future improvement, gives police the power to gather information that is the “modern-day equivalent” of activity that has been held to be a Fourth Amendment search, the use of that technology is also a search.¹⁶ This is a far simpler and more straightforward test to apply than the multi-factor core test of *Carpenter*, and for that reason, could end up becoming the *Carpenter* rule cited most often as the basis for requiring the police to get a warrant.

The last revolution is a revolution of legal reasoning. In his opinion, the Chief Justice evinces, as he did in the majority opinion in *Riley v. California*,¹⁷ a profound *tech exceptionalism*.¹⁸ Recent advances in information technology are different in kind, not merely in degree from what has come before. This idea finds substantial support in two decades of legal scholarship about threats from technology to information privacy, work that has never before received such a profound endorsement from the Supreme Court.

In embracing tech exceptionalism, the Court expressly declined invitations from scholars and amici to base its Fourth Amendment reasoning in traditional disciplines such as history or economics.¹⁹ Scholars coming from those interdisciplinary traditions have expressed disappointment about this choice, which is an understandable reaction to having been heard and rejected.²⁰

Carpenter is an inflection point in the history of the Fourth Amendment. From now on, we will be talking about what the Fourth Amendment means in pre-*Carpenter* and post-*Carpenter* terms. It will be considered as important as *Olmstead*²¹ and *Katz*²² in the overall arc of technological privacy.²³

This article proceeds in three parts. Part II first lays out the new rule of *Carpenter*, which protects large databases full of information from unreasonable police access according to a new, multi-factor test, and then applies the test to private databases of information beyond the one at issue in the case. Part III explains how *Carpenter* has turned the government action rule of the Fourth Amendment on its head and cre-

16. See *Carpenter*, 138 S. Ct. at 2222 (calling Justice Kennedy’s “modern-day equivalent” discussion a “sensible exception”); *id.* at 2230 (Kennedy, J., dissenting).

17. 134 S. Ct. 2473 (2014).

18. See *infra* Section IV.B.

19. See *infra* Section IV.F.

20. *Id.*

21. *Olmstead v. United States*, 277 U.S. 438 (1928) (holding that a wiretap is not a search, embracing the trespass theory of the Fourth Amendment).

22. *Katz v. United States*, 389 U.S. 347, 351 (1967) (holding that placing a recording device on the exterior of a telephone booth is a search).

23. See *infra* Section III.A.

ated three new rules of technological equivalence. Finally, Part IV discusses the tech exceptionalism at the heart of *Carpenter* and how it changes Fourth Amendment reasoning.

II. THE NEW RULE OF CARPENTER

Carpenter held that the government collection of CSLI is a search by introducing a new, multi-factor test.²⁴ This test serves the dual purpose of deciding: (1) whether access to large databases full of personal information about individuals constitutes a search under the Fourth Amendment and (2) whether the third-party doctrine should extend to such access.²⁵

The Court did not exhaustively specify or defend the new test, although a close reading of the opinion reveals the critical factors and why they matter.²⁶ When the police seek to obtain information about individual behavior contained in a private party's database, the court examines (1) "the deeply revealing nature" of the information; (2) "its depth, breadth, and comprehensive reach"; and (3) "the inescapable and automatic nature of its collection."²⁷ The importance of these factors finds great support in recent legal scholarship.²⁸ When lower courts apply these factors, they are likely to extend the Fourth Amendment to cover many important commercial databases that have never before required a warrant for the police to access.

A. *Carpenter's Broad New Rule*²⁹

Carpenter held that the police may not collect historical CSLI from a cell phone service provider without a warrant.³⁰ Footnote three restricted the holding, for now, to seven days of collection.³¹

24. *Carpenter v. United States*, 138 S. Ct. 2206, 2223 ("In light of the deeply revealing nature of CSLI, its depth, breadth, and comprehensive reach, and the inescapable and automatic nature of its collection, the fact that such information is gathered by a third party does not make it any less deserving of Fourth Amendment protection.").

25. *See id.*

26. *See infra* Section II.C.

27. *Carpenter*, 138 S. Ct. at 2223 (emphasis added).

28. *See infra* Section III.C (connecting each of the *Carpenter* factors to recent legal scholarship).

29. This subpart is adapted from a blog post I authored shortly after the *Carpenter* decision was handed down. *See* Paul Ohm, *The Broad Reach of Carpenter v. United States*, JUST SECURITY (June 27, 2018), <https://www.justsecurity.org/58520/broad-reach-carpenter-v-united-states> [https://perma.cc/2FL2-KPSS].

30. *Carpenter*, 138 S. Ct. at 2217.

31. *Id.* at 2217 n.3.

This is the opinion most privacy law scholars and privacy advocates have been awaiting for decades.³² Oceans of ink have been spilled by those worried about how the dramatic expansion of technologically fueled corporate surveillance of our private lives automatically expands police surveillance too, thanks to the way the Supreme Court has construed the reasonable expectation of privacy test and the third-party doctrine.³³ The Fourth Amendment protects only that which is protected by a “reasonable expectation of privacy” (“REP”).³⁴ This requires a two-pronged analysis, “first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as ‘reasonable.’”³⁵ The third-party doctrine says that information a person voluntarily discloses to a third party is not protected by a reasonable expectation of privacy.³⁶

With *Carpenter*, the Supreme Court reinvents the REP test. Until now, the Supreme Court has tended to pay more attention to the nature of the police intrusion required to obtain information than to the nature of the information obtained. Information has been deemed protected by REP because the police obtained it using advanced thermal imaging tools,³⁷ or a wireless beeper located inside a house.³⁸ Information has

32. DAVID GRAY, *THE FOURTH AMENDMENT IN AN AGE OF SURVEILLANCE* 17 (2017) (“The task for the Court in our age of surveillance is to fashion new Fourth Amendment remedies to meet twenty-first-century challenges.”); DANIEL J. SOLOVE, *NOTHING TO HIDE: THE FALSE TRADEOFF BETWEEN PRIVACY AND SECURITY* 2 (2011) (“When evaluating security measures, judges are often too deferential to security officials. And the law gets caught up in cumbersome tests to determine whether government information gathering should be subjected to oversight and regulation, resulting in uneven and incoherent protection.”); Susan Freiwald, *Cell Phone Location Data and the Fourth Amendment: A Question of Law, Not Fact*, 70 MD. L. REV. 681, 746 (2011) (advocating for judicial determination that individuals have an objectively reasonable expectation of privacy in location information) [hereinafter Freiwald, *Cell Phone Location Data*].

33. See, e.g., Susan Freiwald, *First Principles of Communications Privacy*, 2007 STAN. TECH. L. REV. 3 at *49 (2007) (“By focusing merely on whether third parties have access to our communications data, or whether that data can be characterized as non-contents, courts have authorized increasingly powerful surveillance methods without meaningful judicial oversight.”) [hereinafter Freiwald, *First Principles*]; David Gray & Danielle Citron, *The Right to Quantitative Privacy*, 98 MINN. L. REV. 62, 139–40 (2013) (“The implications for Fourth Amendment interests in quantitative privacy are obvious. What the government cannot collect or aggregate directly, it can simply get from third parties with whom the information has been shared.”); Neil Richards, *The Third-Party Doctrine and the Future of the Cloud*, 94 WASH. U.L. REV. 1441, 1482 (2017) (“If we accept the logic of the Third-Party Doctrine for our current data practices, then it would logically follow that future data sets would also lose Fourth Amendment protection.”).

34. *Katz v. United States*, 389 U.S. 347, 360–61 (1967) (Harlan, J., concurring) (articulating the reasonable expectation of privacy test).

35. *Id.*

36. See Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 566–70 (2009).

37. *Kyllo v. United States*, 533 U.S. 27, 34–35 (2001).

38. *United States v. Karo*, 468 U.S. 705, 714–15 (1984).

fallen outside an REP when obtained from trash left on the curb,³⁹ low-flying aircraft,⁴⁰ or a wireless beeper traveling on public roads.⁴¹ The analysis has almost always turned primarily on the invasion and only secondarily on the information.

Carpenter heralds a new mode of Constitutional analysis because the Court finds an REP based largely on an analysis of the information divorced from the actions of the police, database owner, or surveillance target. The most important holding — which commanded the votes of five justices — is that “individuals have a reasonable expectation of privacy in the whole of their physical movements.”⁴² The Court explains that a database full of CSLI meets this standard using an analysis focused exclusively on the nature of the data in the database and the target’s role in its initial collection.

Next, with *Carpenter*, the third-party doctrine appears to be nearly dead. The majority opinion “decline[d] to extend” the third-party doctrine to the FBI’s collection of seven days of CSLI from cell phone service providers.⁴³ “Given the unique nature of cell phone location information, the fact that the Government obtained the information from a third party does not overcome *Carpenter*’s claim to Fourth Amendment protection.”⁴⁴

Even on their own terms, these two holdings have sweeping consequences for privacy and law enforcement. But it is the manner in which Chief Justice Roberts reasoned his way to them that assures that this opinion will be applied far beyond the facts of this case.

First, as described in the majority and dissenting opinions, the CSLI that has just been protected is not terribly precise.⁴⁵ If the majority had placed an exaggerated gloss on the precision of CSLI at issue in this case, it would have given the government a way in future cases to distinguish other types of location information: “the data at issue in this case is not controlled by *Carpenter*,” the government could have argued, “because it is far less precise than CSLI.”

But, it will be difficult to make this argument because the majority opinion informs us that the CSLI records in this case “placed [*Carpenter*] within a wedge-shaped sector ranging from one-eighth to four square miles.”⁴⁶ In his dissent, Justice Kennedy characterized these dimensions as “covering between a dozen and several hundred city

39. *California v. Greenwood*, 486 U.S. 35, 40 (1988).

40. *Florida v. Riley*, 488 U.S. 445, 450 (1989).

41. *United States v. Knotts*, 460 U.S. 276, 281–82 (1983).

42. *Carpenter v. United States*, 138 S. Ct. 2206, 2217 (citing *United States v. Jones*, 565 U.S. 400, 430 (2012) (Alito, J., concurring); *id.* at 415 (Sotomayor, J., concurring)).

43. *Carpenter*, 138 S. Ct. at 2220.

44. *Id.*

45. *Id.* at 2218.

46. *Id.*

blocks” in cities and “up to 40 times more imprecise” in rural areas.⁴⁷ GPS this certainly is not. The Chief Justice waves this away, in part, because “the rule this Court adopts ‘must take account of more sophisticated systems that are already in use or in development.’”⁴⁸

Second, the majority opinion is not restricted to CSLI. Instead, this is an opinion about information the police can use to locate people generally, not CSLI specifically.⁴⁹ Part IV of the opinion is all about the privacy interests individuals have in “the whole of their physical movements.”⁵⁰ This is a meditation on the nature of location information, whatever form it takes. Geolocation information, when there is enough of it, “provides an intimate window into a person’s life,” quoting Justice Sotomayor’s celebrated opinion from *Jones*, revealing “familial, political, professional, religious, and sexual associations.”⁵¹ This case is “not about ‘using a phone’ . . . [i]t is about a detailed chronicle of a person’s physical presence compiled every day, every moment, over several years.”⁵² It is about “a trail of location data.”⁵³

By focusing on the nature of the information rather than on the telecommunications nitty-gritty used to gather the information or the structure of the database in which the information was held, this opinion provides analysis that should apply to other massive collections of historical geolocation information, of which there are many. Many smartphone apps collect precise GPS information, including apps that have no need for this kind of information except to sell to advertisers.⁵⁴ It is not just your smartphone, as GPS information is gathered by the companies that provide fitness trackers, connected cars, and smart watches. Internet of Things gizmos can place location trackers on our clothes, bags, and even our bodies.⁵⁵ It might not be that every database

47. *Id.* at 2225 (Kennedy, J., dissenting).

48. *Id.* at 2218–19 (quoting *Kyllo v. United States*, 533 U.S. 27, 36 (2001)).

49. *Id.* at 2217–18.

50. *Id.* at 2217 (citing *United States v. Jones*, 565 U.S. 400, 430 (2012) (Alito, J., concurring); *id.* at 415 (Sotomayor, J., concurring)).

51. *Carpenter*, 138 S. Ct. at 2217 (quoting *United States v. Jones*, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring)).

52. *Id.* at 2220.

53. *Id.*

54. See, e.g., KENNETH OLMSTEAD & MICHELLE ATKINSON, PEW RESEARCH CENTER, APP PERMISSIONS IN THE GOOGLE PLAY STORE 22 (2015), http://assets.pewresearch.org/wp-content/uploads/sites/14/2015/11/PI_2015-11-10_apps-permissions_FINAL.pdf [<https://perma.cc/GQ3Y-RPP2>] (finding that in 2014, 24% of apps in the Google Play store requested access to precise GPS location information, while 21% asked for approximate location information); Press Release, Fed. Trade Comm’n, Android Flashlight App Developer Settles FTC Charges It Deceived Consumers (Dec. 5, 2013), <https://www.ftc.gov/news-events/press-releases/2013/12/android-flashlight-app-developer-settles-ftc-charges-it-deceived> [<https://perma.cc/TX29-JZAQ>] (announcing settlement of case against flashlight app manufacturer for sharing precise geolocation information with third parties, thwarting consumer expectations).

55. See, e.g., OFFICE OF SEN. ED MARKEY, TRACKING & HACKING: SECURITY & PRIVACY GAPS PUT AMERICAN DRIVERS AT RISK 8 (2015), <https://www.markey.senate.gov/imo/>

of location information generated by every technology listed above will fall within the *Carpenter* reasoning, but the police should think twice before trying to collect any of it without a warrant.

Third, the majority opinion will probably even apply to information that does not expressly reveal location but from which location may be inferred. “[T]he Court has already rejected the proposition that ‘inference insulates a search,’”⁵⁶ quoting *Kyllo* once again. The opinion highlights how the government could use CSLI “in combination with other information, [to] deduce a detailed log of Carpenter’s movements.”⁵⁷ Many databases that do not store location information directly can be used to infer location information. Credit card records, automatic toll transponder records, automated license-plate records, etc., can all generate inferences about a person’s location that are far more precise than CSLI.⁵⁸ Any time the government accesses a privately assembled database in order to track location over time without a warrant, it risks suppression under *Carpenter*.

media/doc/2015-02-06_MarkeyReport-Tracking_Hacking_CarSecurity%202.pdf [https://perma.cc/4VQH-22GE] (describing collection and transmission of driving history from connected cars); Damon Beres, *These High-Tech Shirts And Pants Can Help Protect Kids With Autism*, THE HUFFINGTON POST (last updated Dec. 6, 2017), https://www.huffingtonpost.com/2015/02/18/autism-gps-device_n_6705368.html [https://perma.cc/4VQH-22GE] (describing location tracking in clothing for autistic children); Carey Dunne, *Forget Fitbits: This T-Shirt Embeds Fitness Sensors Into Its Fabric*, FAST COMPANY (Mar. 6, 2014), https://www.fastcompany.com/3027278/forget-fitbits-this-t-shirt-embeds-fitness-sensors-into-its-fabric [https://perma.cc/GLN8-4B4K] (describing location tracking in exercise clothing); Lisa Eadicicco, *A New Wave Of Gadgets Can Collect Your Personal Information Like Never Before*, BUS. INSIDER (Oct. 9, 2014, 11:26 AM), https://www.businessinsider.com/privacy-fitness-trackers-smartwatches-2014-10 [https://perma.cc/J2Q3-ZTZ7] (describing location tracking in smartwatches and fitness trackers); Ferguson, *The Smart Fourth Amendment*, *supra* note 7 (discussing Fourth Amendment implications of GPS monitors attached to the body); Melanie Swan, *Sensor Mania! The Internet of Things, Wearable Computing, Objective Metrics, and the Quantified Self 2.0*, 1 J. SENSOR & ACTUATOR NETWORKS 217, 221 (2012) (describing GPS monitoring in at least one wristband sensor). Cf. Yael Grauer, *A practical guide to microchip implants*, ARS TECHNICA (Jan. 3, 2018, 7:30 AM), https://arstechnica.com/features/2018/01/a-practical-guide-to-microchip-implants [https://perma.cc/QAG6-YBKB] (describing transponder implants in humans but not referring to GPS).

56. *Carpenter*, 138 S. Ct. at 2218 (quoting *Kyllo v. United States*, 533 U.S. 27, 36 (2001)).

57. *Id.*

58. *See, e.g.*, *United States v. Kragness*, 830 F.2d 842, 865 (8th Cir. 1987) (describing government’s use of credit-card records to prove defendant’s travel history); *In re U.S. for Historical Cell Site Data*, 724 F.3d 600, 614 n.13 (5th Cir. 2013) (“[W]hen a customer makes a credit card purchase at a store or restaurant, he does not directly convey the location of the transaction to his credit card company. Nevertheless, law enforcement officers can obtain his credit card records from the company with a subpoena . . . and use them to track his location . . .”); Mariko Hirose, *Newly Obtained Records Reveal Extensive Monitoring of E-ZPass Tags Throughout New York*, AM. CIVIL LIBERTIES UNION (Apr. 24, 2015, 1:00 PM), https://www.aclu.org/blog/privacy-technology/location-tracking/newly-obtained-records-reveal-extensive-monitoring-e-zpass [https://perma.cc/3BXX-5N7Z] (describing location tracking through toll transponders); Reepal S. Dalal, Note, *Chipping away at the Constitution: The Increasing Use of RFID Chips Could Lead to an Erosion of Privacy Rights*, 86 B.U. L. REV. 485, 494–95 (2006) (discussing the Fourth Amendment implications of toll collection data); AM. CIVIL LIBERTIES UNION, YOU ARE BEING TRACKED: HOW LICENSE PLATE READERS ARE BEING USED TO RECORD AMERICANS’ MOVEMENTS 7 (2013),

This gives the lie to something the majority said that has puzzled commenters: “We do not . . . call into question conventional surveillance techniques and tools, such as security cameras.”⁵⁹ What the Chief Justice misses in this simple statement is how facial recognition technology has advanced to the point that a huge archive of security camera footage can easily be transformed into a massive database tracking the location of identified individuals.⁶⁰ It might be that CSLI records track location far more comprehensively than security camera footage connected to facial recognition software — we will examine the role of the comprehensiveness below⁶¹ — but the majority cannot literally mean that security camera footage is categorically not a search given the reasoning of the opinion.

In sum, criminal defendants will test the outer boundaries of *Carpenter*’s reasoning whenever the police use massive databases assembled by private parties that reveal location information, directly or by inference. Other defendants will challenge the collection of data unrelated to location. The broad reasoning of the majority’s opinion will give all of them plenty to work with. Anticipating this, risk-averse police departments will err on the side of caution, getting a warrant for data whenever they can, sometimes turning promising leads into dead ends. It’s a powerful reminder of the ability the Supreme Court has to protect civil liberties and reshape the contours of our relationship with the state.

B. On Police Efficiency and Time Machines

At the outset of his opinion, the Chief Justice frames two overarching purposes for the Fourth Amendment: “to secure ‘the privacies of life’ against ‘arbitrary power’” and “to place obstacles in the way of a too permeating police surveillance.”⁶² The majority’s opinion is centrally preoccupied with the way technology has made the police more efficient. The opinion returns repeatedly to the idea that this increased efficiency has Fourth Amendment import.

<https://www.aclu.org/files/assets/071613-aclu-alprreport-opt-v05.pdf> (describing location tracking through license-plate records) [<https://perma.cc/2ANN-4654>]; *infra* note 212 (discussing Fourth Amendment implications of license plate readers).

59. *Carpenter*, 138 S. Ct. at 2220.

60. GARVIE ET AL., THE PERPETUAL LINE-UP: UNREGULATED POLICE FACE RECOGNITION IN AMERICA 22 (2016), <https://www.perpetuallineup.org/sites/default/files/2016-12/The%20Perpetual%20Line-Up%20-%20Center%20on%20Privacy%20and%20Technology%20at%20Georgetown%20Law%20-%2020121616.pdf> [<https://perma.cc/5K99-H27P>] (“describing facial recognition software used by law enforcement agencies for purposes including geolocation”).

61. *Infra* Section II.C.

62. *Carpenter*, 138 S. Ct. at 2214 (first quoting *Boyd v. United States*, 116 U.S. 616, 630 (1886); and then quoting *United States v. Di Re*, 332 U.S. 581, 595 (1948)).

The idea of police efficiency is given one particularly evocative and salient analogy: crime fighting time machines. A key distinction between CSLI and other location tracking methods from history is the fact that with CSLI, everyone is being tracked at all times, long before any one of us falls under the scrutiny of the police. The metaphor of police access to historical data as time travel was first proposed by legal scholar Stephen Henderson.⁶³

There are, however, two ways to read this attention to police efficiency gain: First, this might be what connects the *Carpenter* holding to *Katz*. Members of society do not expect the gains in efficiency of the police, and it is this misalignment in our expectations that leads to the conclusion that a search has occurred:

Prior to the digital age, law enforcement might have pursued a suspect for a brief stretch, but doing so “for any extended period of time was difficult and costly and therefore rarely undertaken.” For that reason, “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.” . . . And like GPS monitoring, cell phone tracking is remarkably easy, cheap, and efficient compared to traditional investigative tools. With just the click of a button, the Government can access each carrier’s deep repository of historical location information at practically no expense.⁶⁴

The two internal quotes come from Justice Alito’s concurrence in *Jones*, which also placed great weight on preventing the power of the police to increase dramatically through the progress of technology.⁶⁵

The second way to read the *Carpenter* court’s focus on increased police efficiency treats the Fourth Amendment as a constitutional lever. This interpretation can require the police to be more inefficient than modern technology would otherwise allow, by forcing the police to stop and get a warrant. The court, quite strikingly, recited near the very beginning of its discussion of the doctrine that a “central aim of the Framers was ‘to place obstacles in the way of a too permeating police surveillance.’”⁶⁶

63. Stephen E. Henderson, *Fourth Amendment Time Machines (and What They Might Say About Police Body Cameras)*, 18 U. PENN. J. CON. L. 933, 935 (2016).

64. *Carpenter*, 138 S. Ct. at 2217–18 (internal citations omitted).

65. *United States v. Jones*, 565 U.S. 400, 429–430 (2012) (Alito, J., concurring).

66. *Carpenter*, 138 S. Ct. at 2214.

There is a subtle but important difference in these two approaches. The former is a less interventionist, more reactive role for the judiciary going forward: the judge's role is to note those moments when public expectation diverges from technological reality and to temporarily slow things down. Presumably, at some point society's expectations will catch up to the technologically possible; at some point we will recognize that we live in an age of technologically abetted super police. At that moment, the passive approach would suggest, we can dispense with the warrant requirement in this case.

In contrast, the latter assigns a far more interventionist and proactive role for judges. As stated in *Carpenter* above, the role of judges is to "place obstacles in the way of a too permeating police surveillance." This suggests a much more long-lived state of affairs. Warrants are required to add friction in the way of our technologically abetted super police. Even if society begins to expect a more efficient police force, the police will still be required to subject itself to the twin ordeals of probable cause and judicial review.

To put it more colloquially, the former approach is like a speed bump, while the latter is like a road block. In either event, *Carpenter* puts to rest the dictum in *United States v. Knotts*⁶⁷ that "[w]e have never equated police efficiency with unconstitutionality, and we decline to do so now."⁶⁸

Time — and further case law development — will tell which of these interpretations controls after *Carpenter*. I prefer the more interventionist version: the Fourth Amendment should be seen as a road-block to a hyper-efficient police force. It should require warrants not only until society grows accustomed to powerful new forms of surveillance; warrant requirements must have a more lasting and durable lifespan. The interventionist interpretation also finds support from a broad range of legal scholarship.⁶⁹ Of most direct relevance, it stems from an important article by Kevin Bankston and Ashkan Soltani.⁷⁰ They argue that the police engage in a Fourth Amendment search whenever a new technology makes it "much less expensive" to collect information about individuals.⁷¹ The article presents a compelling case that the facts of *Jones* meets this standard, because a police-installed GPS

67. *United States v. Knotts*, 460 U.S. 276 (1983).

68. *Id.* at 284.

69. See, e.g., Luke M. Milligan, *Analogy Breakers: A Reality Check on Emerging Technologies*, 80 MISS. L.J. 1319, 1337 (2011) (arguing that the increased efficiency of the government should be a factor in considering whether a court should engage in a "fresh" analysis of a legal doctrine).

70. Kevin S. Bankston & Ashkan Soltani, *Tiny Constables and the Cost of Surveillance: Making Cents Out of United States v. Jones*, 123 YALE L.J. ONLINE 335 (2014), <http://yalelawjournal.org/forum/tiny-constables-and-the-cost-of-surveillance-making-cents-out-of-united-states-v-jones> [<https://perma.cc/NBL9-PN59>].

71. *Id.* at 337.

tracker significantly reduces the cost of location tracking. They lend rigor to this conclusion by meticulously reading FBI pursuit manuals and cross-referencing them to FBI Special Agent salary tables to conclude that a GPS tracker is twenty-eight times cheaper than covert pursuit, while tracking location by cell phone — akin to the facts of *Carpenter* — is almost twice as cheap as GPS tracking.⁷²

Bankston and Soltani pay due to other scholarship, most importantly Orin Kerr's theory of equilibrium adjustment.⁷³ According to this influential theory, "[w]hen new tools and new practices threaten to expand or contract police power in a significant way, courts adjust the level of Fourth Amendment protection to try to restore the prior equilibrium."⁷⁴ *Carpenter* is the ultimate embrace of both the Bankston-Soltani theory of efficiency and the Kerr theory of equilibrium adjustment.⁷⁵

Whether the Court intended the weaker or stronger approach to responding to police efficiency will dictate how long we will be governed by particular warrant requirements. But at least in the short term, what emerges is the same three-factor test.

C. What is the Carpenter Test?

The test that emerges from the majority opinion will also be applied to collections of information maintained by third parties that do not track location, not even by inference, but are of interest to law enforcement. Going forward, whenever the government obtains a copy of a massive database of information containing non-public information about individuals, judges will conduct a qualitative and quantitative assessment of the information, using a new, multi-factor test. This assessment will answer two questions: First, does the individual whose information has been obtained have a reasonable expectation of privacy in the database? Second, even if that information has been collected and

72. *Id.* at 354 (depicting visually the efficiency multipliers of using technology to track location as opposed to manual surveillance).

73. *Id.* at 337–38 n.10 (citing Orin S. Kerr, *An Equilibrium-Adjustment Theory of the Fourth Amendment*, 125 HARV. L. REV. 476 (2011) [hereinafter Kerr, *Equilibrium*]). They also generously connect it to my earlier writing. *Id.* at 337 n.11 (citing Paul Ohm, *The Fourth Amendment in a World Without Privacy*, 81 MISS. L.J. 1309, 1312 (2012)). The final building block is the work of Harry Surden, *Structural Rights in Privacy*, 60 SMU L. REV. 1605 (2007).

74. Kerr, *Equilibrium*, *supra* note 73, at 480.

75. See Orin Kerr, *Understanding the Supreme Court's Carpenter Decision*, LAWFARE (June 22, 2018, 1:18 PM), <https://www.lawfareblog.com/understanding-supreme-courts-carpenter-decision> [<https://perma.cc/A4LD-5V8K>] (arguing that the majority opinion embraces equilibrium-adjustment theory). No less than Edward Snowden has embraced this reading. Edward Snowden (@Snowden), TWITTER (June 22, 2018, 9:23 AM), <https://twitter.com/Snowden/status/1010196684066959360> [<https://perma.cc/9C24-8GJY>] ("The Bankston-Soltani Principle is alive and well.").

is being maintained by a private third party, does the third-party doctrine apply?

There is likely to be disagreement about the precise list of *Carpenter* factors, given the wide-ranging nature of the opinion. Different characteristics of CSLI data and smartphone use are emphasized throughout Chief Justice Roberts's opinion.⁷⁶ Still, in concluding the opinion, he helpfully isolates three factors: (1) "the deeply revealing nature" of the information; (2) "its depth, breadth, and comprehensive reach"; and (3) "the inescapable and automatic nature of its collection."⁷⁷

Later, I will say even more about the theoretical foundations and normative desirability of this test,⁷⁸ but for now, let us note the similarity of the test to the work of Susan Freiwald.⁷⁹ Freiwald has long advocated that the Court embrace her own four-factor test for deciding whether there is an invasion of REP in electronic surveillance.⁸⁰ She argues that courts should inquire whether the police are using a "hidden, intrusive, indiscriminate, and continuous method of surveillance."⁸¹ Using this test, she bested the Supreme Court by seven years, arguing in 2011 that the police should be required to obtain a warrant to access CSLI.⁸²

Let us consider each of the *Carpenter* factors in turn. The sections that follow will highlight the key language from the majority opinion about each factor, as well as focus on language from the various dissents that sharpen the meaning or import of each factor. These sections will also connect most of the factors to the broader world of privacy law and scholarship beyond this case. This is meant to address a criticism that has been directed at the majority's opinion: its failure to cite any legal scholarship.⁸³ The Court could have supported each of its points with scholarly citation. However, this opinion still resonates with two decades of writing about the Fourth Amendment in an age of rapidly changing technology, regardless of whether the Chief Justice was aware of any of this work. Consider this the majority's missing cite check, demonstrating the rigor and theoretical underpinnings of this approach.

76. *Carpenter v. United States*, 138 S. Ct. 2206, 2216–20 (2018).

77. *Id.* at 2223.

78. See *infra* Parts III–IV.

79. See Susan Freiwald, *Cell Phone Location Data and the Fourth Amendment: A Question of Law, Not Fact*, 70 MD. L. REV. 681, 746 (2011) [hereinafter Freiwald, *Cell Phone Location Data*]; Freiwald, *First Principles*, *supra* note 33.

80. Freiwald, *First Principles*, *supra* note 33; *infra* Section IV.B (explaining and defending the four-factor test).

81. Freiwald, *First Principles*, *supra* note 33 at *50.

82. Freiwald, *Cell Phone Location Data*, *supra* note 79, at 746–48.

83. See, e.g., Strahilevitz & Tokson, *Ten Thoughts*, *supra* note 2.

1. First Factor: Deeply Revealing Nature

The *Carpenter* test protects information only if it is “deeply revealing” of some private quality of the person under surveillance.⁸⁴ “As with GPS information, the time-stamped data provides an intimate window into a person’s life, revealing not only his particular movements, but through them his ‘familial, political, professional, religious, and sexual associations.’”⁸⁵ These location records ‘hold for many Americans the privacies of life.’”⁸⁶

To give labels to these requirements, information stored by a private third party must in some way be deemed sensitive or intimate to fall within the reasonable expectation of privacy test. These two words, although similar to one another, have different meanings. Sensitive information is information that can be used to cause an individual or group harm.⁸⁷ In contrast, intimate information reveals something important and not widely known about a relationship between individuals.⁸⁸

The connection between sensitive and intimate information and the REP test has a long doctrinal lineage. Professor Orin Kerr argues that the Supreme Court has adopted four different models for assessing whether police practice implicates a reasonable expectation of privacy, one of which is a “private facts” model. This model measures the sensitivity and intimacy of the information obtained.⁸⁹

The road to the Court’s recognition of the “deeply revealing nature” factor was paved by the two blockbuster opinions from recent years about technology and the Fourth Amendment, *United States v. Jones* and *Riley v. California*.⁹⁰ The notion that detailed location information can reveal one’s “familial, political, professional, religious, and sexual associations” comes from Justice Sotomayor’s concurrence in *Jones*,⁹¹ perhaps the single most important quote ever uttered in a Supreme Court opinion about the sensitivity of information. The idea that a smart phone can “hold for many Americans, the ‘privacies of life’” comes from Chief Justice Roberts’s opinion in *Riley*.⁹²

84. *Carpenter v. United States*, 138 S. Ct. 2206, 2223 (2018).

85. *Id.* at 2217 (quoting *United States v. Jones*, 565 U.S. 400, 415 (2012)) (citations and internal quotation marks omitted).

86. *Id.* (quoting *Riley v. California*, 134 S. Ct. 2473, 2495 (2014)) (citations and internal quotation marks omitted).

87. See Paul Ohm, *Sensitive Information*, 88 S. CAL. L. REV. 1125, 1133–34 (2015) [hereinafter Ohm, *Sensitive Information*].

88. See JULIE C. INNESS, *PRIVACY, INTIMACY, AND ISOLATION* 56–57 (1992).

89. Orin S. Kerr, *Four Models of Fourth Amendment Protection*, 60 STAN. L. REV. 503, 512–15 (2007) [hereinafter Kerr, *Four Models*]. The other three models are “probabilistic,” “positive law,” and “policy.” *Id.* at 506. We will return to this later.

90. 565 U.S. 400 (2012); 134 S. Ct. 2473 (2014).

91. *Jones*, 565 U.S. at 415 (Sotomayor, J., concurring).

92. *Riley*, 134 S. Ct. at 2494–95 (quoting *Boyd v. United States*, 116 U.S. 616, 630 (1886)).

As discussed earlier, this factor focuses exclusively on an analysis of the intrinsic nature of the information itself, divorced from any consideration of what the police had to do to obtain it, the company's incentives for gathering it, or what the individual could have done to prevent it. *Carpenter* is a fundamental break from most Fourth Amendment analyses of the past, which almost always placed police action and individual counter-action at the center, and information on the periphery.

2. Second Factor: Depth, Breadth, and Comprehensive Reach

The *Carpenter* test protects information that possesses “depth, breadth, and comprehensive reach.”⁹³ Like the first factor, the second factor focuses on the intrinsic nature of the information.

Justice Kennedy, in dissent, provided his own list of the factors he saw in the majority's opinion, to criticize the majority's “unstable foundation.”⁹⁴ Of the factors in his list, the one that most closely resembles “depth, breadth, and comprehensive reach” is a single factor, “comprehensiveness,”⁹⁵ but it is better to treat this as comprising three distinct requirements (meaning our three factors might instead be treated as five). All three primarily speak to the quantity of information stored. But they measure a database along three distinct dimensions.

Depth refers to the detail and precision of the information stored.⁹⁶ This is closely related to the deeply revealing nature factor, as it is the precision of location information that triggers Justice Sotomayor's litany of private inferences — location information betrays a person's “familial, political, professional, sexual, religious, and sexual associations” only if it is sufficiently precise to imply visits to particular storefronts, homes, or other individual locations.⁹⁷ The *Carpenter* majority emphasizes that CSLI stores “the whole of [a person's] physical movements”⁹⁸ as well as “a detailed chronicle of a person's physical presence.”⁹⁹

In contrast, *breadth* refers to time in two ways: how frequently the data is collected, and for how long the data has been recorded.¹⁰⁰ CSLI

93. *Carpenter v. United States*, 138 S. Ct. 2206, 2223 (2018).

94. *Id.* at 2234 (Kennedy, J., dissenting).

95. *Id.*

96. *See id.* at 2218 (majority opinion) (“From the 127 days of location data it received, the Government could, in combination with other information, deduce a detailed log of Carpenter's movements, including when he was at the site of the robberies. And the Government thought the CSLI accurate enough to highlight it during the closing argument of his trial.”).

97. *Id.* at 2217 (quoting *United States v. Jones*, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring)).

98. *Id.* at 2219.

99. *Id.* at 2220.

100. *See id.* at 2212 (“Altogether the Government obtained 12,898 location points cataloging Carpenter's movements — an average of 101 data points per day.”).

qualifies as broad in both senses, because the database at issue in *Carpenter* stored “an average of 101 data points per day” of the defendant’s location,¹⁰¹ and because cell phone providers tend to store data for up to five years.¹⁰² Every one of us “has effectively been tailed every moment of every day for five years.”¹⁰³ It is information “compiled every day, every moment, over several years.”¹⁰⁴

Finally, *comprehensive reach* refers to the number of people tracked in the database.¹⁰⁵ This recognizes that there, but by the grace of the police, go I. “Critically, because location information is continually logged for all of the 400 million devices in the United States — not just those belonging to persons who might happen to come under investigation — this newfound tracking capacity runs against everyone.”¹⁰⁶ This is critical because, “[u]nlike with the GPS device in *Jones*, police need not even know in advance whether they want to follow a particular individual, or when.”¹⁰⁷ By identifying these factors in *Carpenter*, the Court in effect endorses the mosaic theory of privacy.¹⁰⁸ The mosaic theory is animated by an idea that finds support both in folk wisdom and modern machine learning: the whole is greater than the sum of the parts.¹⁰⁹ It first found expression in Fourth Amendment jurisprudence in *United States v. Maynard*,¹¹⁰ the D.C. Circuit opinion that was renamed *United States v. Jones* on its way to the Supreme Court. In the majority opinion in *Maynard*, Judge Ginsburg concluded that “[p]rolonged 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.”¹¹¹ Although the *Jones* majority chose not to embrace the mosaic theory, focusing instead on the physical trespass that occurred during the installation of the GPS tracking device,¹¹² *Carpenter* seems to revive the idea.

101. *Id.*

102. *Id.* at 2218.

103. *Id.*

104. *Id.* at 2220.

105. *See id.* at 2218 (“Whoever the suspect turns out to be, he has effectively been tailed every moment of every day for five years, and the police may — in the Government’s view — call upon the results of that surveillance without regard to the constraints of the Fourth Amendment. Only the few without cell phones could escape this tireless and absolute surveillance.”).

106. *Id.*

107. *Id.*

108. *See* Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311, 313–14 (2012) [hereinafter Kerr, *Mosaic Theory*] (defining “mosaic theory” of privacy).

109. *Id.* at 326.

110. 615 F.3d 544 (D.C. Cir. 2010), *aff’d sub nom.* *United States v. Jones*, 565 U.S. 400 (2012).

111. *Id.* at 562.

112. *United States v. Jones*, 565 U.S. 400, 404 (2012).

The mosaic theory brings us to footnote three of *Carpenter*:

The parties suggest as an alternative to their primary submissions that the acquisition of CSLI becomes a search only if it extends beyond a limited period. As part of its argument, the Government treats the seven days of CSLI requested from Sprint as the pertinent period, even though Sprint produced only two days of records. Contrary to Justice KENNEDY's assertion, we need not decide whether there is a limited period for which the Government may obtain an individual's historical CSLI free from Fourth Amendment scrutiny, and if so, how long that period might be. It is sufficient for our purposes today to hold that accessing seven days of CSLI constitutes a Fourth Amendment search.¹¹³

Two of the dissents criticized the seeming arbitrariness of this seven-day rule.¹¹⁴ Footnote three has already sparked scholarly criticism and commentary.¹¹⁵ Any opinion that tries to give force to the mosaic theory has to draw a line.¹¹⁶ Given the role that the quantity factors play in the majority's reasoning, it seems likely that a database containing a single datum that revealed a single registration between a cell phone and cell site would not trigger nearly the same privacy concerns. A single data point would be neither as deep, broad, nor comprehensive, as seven days (much less five years) of CSLI. For that reason, it would not be nearly as "deeply revealing." A future court asked to rule on the warrantless access of a single datum of location information might well distinguish it from the facts and reasoning of *Carpenter*.

While one point of information might not suffice, one should not read too much into the seven-day figure. For one thing, this is the figure that the facts presented: the government sought seven days of CSLI.¹¹⁷ In fact, the order seeking seven days of information elicited only two days of CSLI.¹¹⁸ The Court gave no principled reason for selecting

113. *Carpenter v. United States*, 138 S. Ct. 2206, 2217 n.3 (2018) (citations omitted).

114. *Id.* at 2234 (Kennedy, J., dissenting); *id.* at 2266–67 (Gorsuch, J., dissenting).

115. See, e.g., ORIN S. KERR, *THE DIGITAL FOURTH AMENDMENT* (forthcoming 2019) [hereinafter KERR, *DIGITAL FOURTH AMENDMENT*]; Susan Freiwald & Stephen Wm. Smith, *The Carpenter Chronicle: A Near-Perfect Surveillance*, 132 HARV. L. REV. 205, 228 (2018).

116. Kerr, *Mosaic Theory*, *supra* note 108, at 333–34 (discussing the need to draw lines based on time for a mosaic theory approach to the Fourth Amendment).

117. *Carpenter*, 138 S. Ct. at 2212; see also *id.* at 2217 n.3 (citing the government's suggestion of a seven-day cutoff for CSLI acquisition to become a search).

118. *Id.* at 2212.

seven days as the cut-off, so we ought not consider it the precise dividing line. Future opinions will need to analyze the relationship between the temporal breadth of data and the impact on privacy interests.

These quantitative facts are sure to be the source of confusion in the lower courts — and inside police stations — and the target of criticism from other scholars.¹¹⁹ What if a database has only two forms of quantitative comprehensiveness — say depth and breadth — but about only one person, rather than with comprehensive reach? What if a database reveals deep information about many people, but recorded at a single moment in time?

One potential complicating scenario was expressly referenced in the majority opinion: Does a real-time, future-looking, prospective collection of data trigger this factor and thus the *Carpenter* rule?¹²⁰ The majority opinion expressly declined to say.¹²¹ At the same time, it emphasized repeatedly the retrospective nature of CSLI information, and indeed, Justice Kennedy included “retrospectivity” in his summary of the factors, although the majority opinion did not.¹²² What will lower courts say about real-time CSLI collection?

On the one hand, it is clear that the majority opinion is quite worried about the time-travel nature of the CSLI database, which isn’t implicated in the same way by real-time data gathering.¹²³ Real-time CSLI gathering can be “switched on” for a specific target, allowing it to be pinpointed rather than amassed indiscriminately.

But on the other hand, retrospectivity is just one version of problematic “breadth,” and should be seen as such, rather than being treated as a necessary requirement. There might be databases that collect a broad swath of data across time without being retrospective in the same way as the CSLI database. One example would be a police order commanding a phone company to collect CSLI in real-time about one individual for seven days.¹²⁴ Or consider a database that stores

119. See, e.g., KERR, DIGITAL FOURTH AMENDMENT, *supra* note 115 (arguing that *Carpenter* should not turn on the amount of information obtained).

120. *Carpenter*, 138 S. Ct. at 2220 (declining to express an opinion about “real-time CSLI”).

121. *Id.*

122. *Id.* at 2218 (“With access to CSLI, the Government can now travel back in time to retrace a person’s whereabouts”); *id.* at 2234 (Kennedy, J., dissenting) (listing factors including retrospectivity); *id.* at 2223 (majority opinion) (listing factors not including retrospectivity).

123. *Id.* at 2218. The metaphor of treating police access to historical data as travel in a time machine was first proposed by legal scholar Steven Henderson. Henderson, *supra* note 63, at 935.

124. Compare *Jones v. United States*, 168 A.3d 703, 713 (D.C. 2017) (holding that use of a cell-site simulator to locate a suspect’s phone in real time “invaded a reasonable expectation of privacy and was thus a search”), with *United States v. Riley*, 858 F.3d 1012, 1018 (6th Cir. 2017), *cert. denied*, 138 S. Ct. 2705 (2018) (holding that “government did not conduct a search under the Fourth Amendment when it tracked the real-time GPS coordinates of” suspect’s phone outside the home for seven hours). Other courts avoided answering whether

retrospective information only about some people but not everybody in the database.¹²⁵ So long as the information is deep, broad, and of comprehensive reach, it should trigger this factor, whether or not it is retrospective in the same way.

3. Third Factor: The Inescapable and Automatic Nature of the Collection

The first two factors focus on the information's intrinsic nature. They analyze information as a database designer would, examining the qualitative and quantitative content of the data and the inferences that can be drawn from it. The third factor, in contrast, operates in a much more traditional mode, focusing on what the database owner and data subject have done (or could have done).

The third and final factor is the "inescapable and automatic nature" of how the information is collected.¹²⁶ This factor speaks to whether the targets of the surveillance may have assumed the risk of the data collection or knowingly exposed their information to the private party.¹²⁷ This factor (really two separate factors) brings into the analysis the idea that individuals might sometimes relinquish their Fourth Amendment rights when they assume the risk of surveillance, for example by publishing information to the general public.

Some forms of data collection are *inescapable* because they relate to services one needs to use to be a functioning member of today's society. In the case of CSLI, cell phones are "'such a pervasive and insistent part of daily life' that carrying one is indispensable to

obtaining real-time data constitutes a search. *See, e.g.,* United States v. Wallace, 866 F.3d 605, 609 (5th Cir. 2017), *withdrawn and superseded*, 885 F.3d 806 (5th Cir. 2018) (noting that it is an open question whether it is a search to obtain real-time E911 data but nonetheless holding that police were covered by good-faith exception to exclusionary rule); United States v. Banks, 884 F.3d 998, 1012–13 (10th Cir. 2018) (declining to decide whether "tracking a cell-phone's real-time location is a search" because parties did not thoroughly brief the issue, but, assuming that it was a search, finding exigent circumstances exception applied). *See generally* Eric Lode, Annotation, *Validity of Use of Cellular Telephone or Tower to Track Prospective, Real Time, or Historical Position of Possessor of Phone Under Fourth Amendment*, 92 A.L.R. Fed. 2d 1 (2015).

125. For example, under the USA FREEDOM Act of 2015, the NSA can request telephony metadata records relating to a suspect and everyone within "two hops" of contact with the suspect. 50 U.S.C. § 1861(c)(2)(F)(iii)–(iv) (2012 & Supp. III 2015) (permitting "the prompt production of a first set" and "a second set of call detail records"). Researchers estimate that this can net the records of approximately 25,000 subscribers with a single search. Jonathan Mayer et al., *Evaluating the Privacy Properties of Telephone Metadata*, 113 PROC. NAT'L ACAD. SCI. 5536, 5538 (2016).

126. *Carpenter*, 138 S. Ct. at 2223.

127. *Id.* at 2220 ("Apart from disconnecting the phone from the network, there is no way to avoid leaving behind a trail of location data. As a result, in no meaningful sense does the user voluntarily 'assume[] the risk' of turning over a comprehensive dossier of his physical movements.") (quoting *Smith v. Maryland*, 442 U.S. 735, 745 (1979)).

participation in modern society.”¹²⁸ The *Carpenter* opinion makes this point in dramatic fashion by borrowing from Chief Justice Roberts’s opinion in *Riley*:

Unlike the bugged container in *Knotts* or the car in *Jones*, a cell phone — almost a “feature of human anatomy,” *Riley*, 573 U.S., at —, 134 S. Ct., at 2484 — tracks nearly exactly the movements of its owner. While individuals regularly leave their vehicles, they compulsively carry cell phones with them all the time. A cell phone faithfully follows its owner beyond public thoroughfares and into private residences, doctor’s offices, political headquarters, and other potentially revealing locales. See *id.*, at —, 134 S. Ct., at 2490 (noting that “nearly three-quarters of smart phone users report being within five feet of their phones most of the time, with 12% admitting that they even use their phones in the shower”); contrast *Cardwell v. Lewis*, 417 U.S. 583, 590, 94 S. Ct. 2464, 41 L.Ed.2d 325 (1974) (plurality opinion) (“A car has little capacity for escaping public scrutiny.”).¹²⁹

Perhaps reflecting how some members of modern society feel shackled to these devices, Chief Justice Roberts deploys an especially evocative simile: “when the Government tracks the location of a cell phone it achieves near perfect surveillance, as if it had attached an ankle monitor to the phone’s user.”¹³⁰

Inescapability is not the same as the *automatic* nature of the information collected. CSLI is automatically part of cell service because the records are generated whenever the service is used and there is no meaningful opportunity to opt out.¹³¹

[A] cell phone logs a cell-site record by dint of its operation, without any affirmative act on the part of the user beyond powering up. Virtually any activity on the phone generates CSLI, including incoming calls, texts, or e-mails and countless other data connections that a phone automatically makes when checking for news, weather, or social media updates. Apart from disconnecting the phone from the network, there is no

128. *Carpenter*, 138 S. Ct. at 2220 (quoting *Riley v. California*, 134 S. Ct. 2473, 2484 (2014)).

129. *Id.* at 2218.

130. *Id.*

131. *Id.* at 2220.

way to avoid leaving behind a trail of location data. As a result, in no meaningful sense does the user voluntarily “assume[] the risk” of turning over a comprehensive dossier of his physical movements.¹³²

Once again, lower courts might have difficulty applying this factor to technologies that collect data automatically, but not inescapably — such as mobile apps that are voluntarily installed and can be deleted with one click — or those that do so inescapably, but not automatically — such as a doctor’s manual logging of a consenting patient’s symptoms.

4. The Test

To summarize, *Carpenter* promulgates a new three-factor test that should be applied not necessarily to the specific facts of a case but rather to the category of information being sought. In conducting the test, a court should ask whether a given category of information (1) has a deeply revealing nature; (2) possesses depth, breadth, and comprehensive reach; and (3) results from an inescapable and automatic form of data collection.

D. Applying the Carpenter Test

Under this test, what other databases full of third-party-collected records are likely to be found protected by a reasonable expectation of privacy and fall outside the third-party doctrine? Consider a few examples.

1. Very Likely Covered: Web Browsing Records

I am confident that the *Carpenter* test will extend Fourth Amendment protection to web-browsing records collected by ISPs (or browser or operating system manufacturers). Justice Kennedy raises this prospect, complaining that the majority opinion doesn’t reveal whether the seven-day threshold “should apply to information like IP addresses or website browsing history.”¹³³

Web browsing records possess a deeply revealing nature even if they record only the IP addresses of websites visited.¹³⁴ In 2009, I argued that “[t]he potential inconvenience, embarrassment, hardship, or

132. *Id.*

133. *Id.* at 2234 (Kennedy, J., dissenting).

134. See generally Ohm, *Invasive ISP Surveillance*, *supra* note 9, at 1444.

pain that could result from the trove of data of [ISP] monitoring is limited only by the wickedness of one's imagination."¹³⁵ More recently, I testified to Congress that:

The list of websites an individual visits, available to a [broadband Internet access service] provider even when https encryption is used, reveals so much more than a member of a prior generation would have revealed in a composite list of every book she had checked out, every newspaper and magazine she had subscribed to, every theater she had visited, every television channel she had clicked to, and every bulletin, leaflet, and handout she had read. No power in the technological history of our nation has been able until now to watch us read individual articles, calculate how long we linger on a given page, and reconstruct the entire intellectual history of what we read and watch on a minute-by-minute, individual-by-individual basis.¹³⁶

Similarly, Neil Richards has written about the sensitivity of records of "intellectual privacy" like these.¹³⁷ "Intellectual records — such as lists of Web sites visited, books owned, or terms entered into a search engine — are in a very real sense a partial transcript of the operation of a human mind. They implicate the freedom of thought and the freedom of intellectual exploration."¹³⁸ He argues that First Amendment concerns add a gloss to the Fourth Amendment and so access to records like these should require warrants.¹³⁹

The efficiency gain represented by web-browsing records is profound. Just as CSLI has given the police unprecedented power to track the location of targets at very low costs, web browsing records, for the first time in human history, have given the police access to the reading habits of millions of users with very little expense or effort.¹⁴⁰

The "depth, breadth, and comprehensive nature" factor is sure to be more contestable when applied to web browsing records. This precise question has recently been debated publicly in the Federal Communications Commission, which enacted a sweeping broadband privacy rule in the final days of the Obama administration, only to have

135. *Id.*

136. *FCC Overreach: Examining the Proposed Privacy Rules: Hearing Before the H. Subcomm. on Comm'n & Tech. of the H. Comm. on Energy & Commerce*, 114th Cong. 5 (2016) (statement of Paul Ohm, Professor, Georgetown University Law Center).

137. See generally Neil M. Richards, *Intellectual Privacy*, 87 TEX. L. REV. 387 (2008).

138. *Id.* at 436.

139. *Id.* at 440.

140. *Id.*

Congress roll back the rule in the early days of the Trump administration.¹⁴¹ In those proceedings, ISP lobbyists argued that their view into individual reading habits was far from comprehensive — in *Carpenter*'s terms, they lacked depth and breadth — because individuals surf the web via different ISPs.¹⁴² In the course of a single day, many people surf on their phone, their home broadband connection, and their work connection, using a different ISP for each one.¹⁴³ The police might plausibly argue that this distinguishes web browsing data from CSLI because people tend to carry their cell phone in their pockets or purses throughout the day. Your cell phone works like a passive tracking device, sending pings to the nearest cell tower whenever you are using your phone and sometimes even when you are not.¹⁴⁴

Finally, the police might argue that web browsing records generated by an ISP are not “inescapable and automatic” in the same way as CSLI, because web browsing is both intentional and visible behavior — a record is logged whenever you use your phone or computer's web browser to access the web.¹⁴⁵

Lower courts thus might struggle with the uncertainty inherent in the multi-factor test. ISP-generated web browsing records are much more deeply revealing and represent more of an efficiency gain than CSLI records.¹⁴⁶ Although ISPs are deep, broad, of comprehensive reach, inescapable, and automatic, they might not rise for these factors to the same levels as CSLI.

However, I predict courts will have little difficulty holding that massive databases that record the IP addresses visited by an individual meet the three-factor test, even though a few factors cut in the other direction. Police access to these records will constitute a search and thus, the third-party doctrine will not extend to cover them. Going forward, the police are well-advised to seek records like these only after first obtaining a warrant.

141. See Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, 81 Fed. Reg. 87, 274 (Dec. 2, 2016) (to be codified at 47 C.F.R. pt. 64) (rule as enacted); S.J. Res. 34, 115th Cong. (2017) (joint resolution reversing the rule).

142. Peter Swire et al., *Online Privacy and ISPs: ISP Access to Consumer Data is Limited and Often Less than Access by Others* 24–25 (Feb. 29, 2016) (unpublished paper) (on file with The Institute for Information Security & Privacy at Georgia Tech), http://www.iisp.gatech.edu/sites/default/files/images/online_privacy_and_isps.pdf [<https://perma.cc/EC45-YWSP>].

143. *Id.*

144. *Carpenter v. United States*, 138 S. Ct. 2206, 2211 (2018) (“Most modern devices, such as smartphones, tap into the wireless network several times a minute whenever their signal is on, even if the owner is not using one of the phone's features.”).

145. *Cf. Ohm, Invasive ISP Surveillance*, *supra* note 9, at 1476 (describing the automatic nature of ISP surveillance, but concluding that it is conducted without meaningful consent).

146. *Id.* at 1444; Richards, *supra* note 137, at 436.

2. Most Likely Covered: Massive Collections of Telephone and Bank Records

Perhaps counter-intuitively, the police most likely now need a warrant to obtain massive collections of phone records or bank records, the same category of records held not to require a warrant in the third-party doctrine cases *Smith v. Maryland*¹⁴⁷ and *Miller v. United States*.¹⁴⁸ Even though the Court declined to overturn *Smith* and *Miller*, hints throughout the *Carpenter* opinions suggest that, some day, these two opinions will be narrowed to the facts of those 1970s cases.¹⁴⁹

Bank records and phone records can be as deeply revealing as CSLI. *Carpenter's* dissenting opinions make this plain. Justice Kennedy concludes that “[t]he troves of intimate information the Government can and does obtain using financial records and telephone records dwarfs what can be gathered from cell-site records.”¹⁵⁰ Justice Gorsuch asks, “[w]hy is someone’s location when using a phone so much more sensitive than who he was talking to (*Smith*) or what financial transactions he engaged in (*Miller*)?”¹⁵¹ These passages will be quoted the first time a defendant challenges the warrantless access by the police to large quantities of this kind of information. Say the police use a subpoena to obtain years of credit card transactions or the NSA uses a sub-warrant process to obtain millions of telephone metadata. It is now quite likely that courts will require a warrant for this kind of information, citing *Carpenter's* new test.

These courts will now be able to distinguish *Smith* and *Miller* because modern technology tends to produce databases of telephone or financial information that are far more voluminous and detailed than the records at issue in those 1970s cases. With the ubiquity of credit and the decline of cash, almost every commercial transaction we make ends up in a bank record. These might today include great detail about what has been purchased, or a note by the merchant. Similarly, more communications metadata is being collected by today’s telephones than in the past. Computer storage is much cheaper and easier to access than the paper records of the 1970s, reducing the incentive to ever delete anything.¹⁵²

This shines new light on the dueling 2013 district court opinions that assessed the legality of the NSA’s massive telephony metadata pro-

147. 442 U.S. 735 (1979).

148. 425 U.S. 435 (1976).

149. *Carpenter*, 138 S. Ct. at 2217 (declining to extend but not overturning *Smith* and *Miller*).

150. *Id.* at 2232 (Kennedy, J., dissenting).

151. *Id.* at 2262 (Gorsuch, J., dissenting).

152. See generally VIKTOR MAYER-SCHÖNBERGER, DELETE: THE VIRTUE OF FORGETTING IN THE DIGITAL AGE 62–67 (2011).

gram, one distinguishing *Smith* and the other feeling bound by the precedent. The opinions assessed the legality of the program revealed to the public by Edward Snowden, through which the NSA gathered the non-content phone records, such as the originating and receiving telephone numbers of phone calls made by millions of Americans.¹⁵³ In *Klayman v. Obama*,¹⁵⁴ Judge Richard Leon of the District Court for the District of Columbia held that the telephony program likely violated the Fourth Amendment, expressly declining to follow *Smith*.¹⁵⁵ “[T]he *Smith* pen register and the ongoing NSA Bulk Telephony Metadata Program have so many significant distinctions between them that I cannot possibly navigate these uncharted Fourth Amendment waters using as my North Star a case that predates the rise of cell phones.”¹⁵⁶ Less than two weeks later, Judge William Pauley, in *ACLU v. Clapper*,¹⁵⁷ came to the opposite conclusion, finding that *Smith* controlled.¹⁵⁸ “Because *Smith* controls, the NSA’s bulk telephony metadata collection program does not violate the Fourth Amendment.”¹⁵⁹

History, in the form of *Carpenter*, has been much kinder to Judge Leon. A lower court judge trying to rule today that *Smith* controls would have to work much harder than Judge Pauley had to in distinguishing *Carpenter*. Judge Pauley’s reasoning seemed essentially to be that zero times a massive number is still zero. *Smith* found no protectable Fourth Amendment interest in the numbers dialed by a single telephone customer, and therefore, there must also be no Fourth Amendment interest for the collection of the dialing habits of tens of millions of customers.¹⁶⁰

Carpenter makes clear that the scale of data collection matters.¹⁶¹ Constitutionally meaningful privacy can spring forth when records amass in the millions. Judge Pauley’s reasoning should now be seen as defective, especially held next to Judge Leon’s approach, which anticipated the *Carpenter* reasoning, albeit using different factors and language. Judge Leon offered four reasons to distinguish the NSA program

153. Laura K. Donohue, *Bulk Metadata Collection: Statutory and Constitutional Considerations*, 37 HARV. J.L. & PUB. POL’Y 757, 760 (2014).

154. 957 F. Supp. 2d 1 (D.D.C. 2013), *vacated on other grounds*, 800 F.3d 559 (D.C. Cir. 2015).

155. *Id.* at 37.

156. *Id.*

157. 959 F. Supp. 2d 724 (S.D.N.Y. 2013), *vacated on other grounds*, 785 F.3d 787 (2d Cir. 2015).

158. *Id.* at 752.

159. *Id.*

160. *Id.* (“The fact that there are more calls placed does not undermine the Supreme Court’s finding that a person has no subjective expectation of privacy in telephony metadata.” (citing *Smith v. Maryland*, 442 U.S. 735, 745 (1979))).

161. *Carpenter v. United States*, 138 S. Ct. 2206, 2219 (2018) (“There is a world of difference between the limited types of personal information addressed in *Smith* and *Miller* and the exhaustive chronicle of location information casually collected by wireless carriers today.”).

from the facts of *Smith*. First, *Smith* involved data collected over a shorter time frame — 14 days versus months or years.¹⁶² Second, the detailed program between the NSA and the telephone companies created a far more intertwined relationship than the one-off request in *Smith*.¹⁶³ Third, the NSA had the technological capability “to store and analyze the phone metadata of every telephone user in the United States,” providing perhaps the closest parallel between this opinion and *Carpenter*.¹⁶⁴ Finally, telephony metadata can reveal much more sensitive information than the phone records of the late-1970s.¹⁶⁵

Had Judge Leon’s opinion been written after *Carpenter*, it would have been seen as a direct application of the new opinion. Massive databases of telephony records implicate every one of Chief Justice Roberts’s concerns about CSLI. The NSA’s program implicated the Fourth Amendment, notwithstanding the supposed continued vitality of *Smith*. Just like in *Carpenter* itself, I predict courts would “decline to extend *Smith* and *Miller*” to NSA-scale databases of telephony metadata.¹⁶⁶

3. Uncertain Application: Databases of Medical Records and Genetic Information

The examples covered so far — massive databases of web browsing habits, telephone dialing records, and financial records — each satisfy all, or nearly all, of the three *Carpenter* factors and thus, are likely to be found searches. But other databases of investigatory interest face a far less certain fate under the new test.

Under rules promulgated under the Health Insurance Portability and Accountability Act (“HIPAA”), law enforcement, with a grand jury subpoena, can access medical records stored by a covered provider.¹⁶⁷ Has *Carpenter* upset this rule, rendering this regulatory scheme now unconstitutional? Does a large database of health information now require a warrant to access?

For two of the three *Carpenter* factors, one could argue that medical records deserve as much or even more protection than CSLI. Medical records contain symptoms, diagnoses, and prescriptions — information likely far more deeply revealing than location information.¹⁶⁸ Even compared to owning a smartphone, individuals cannot easily choose to avoid professional medical care, making the production of these records more inescapable and automatic. The breadth and efficiency gain

162. *Klayman v. Obama*, 957 F. Supp. 2d 1, 32 (D.D.C. 2013).

163. *Id.* at 32–33.

164. *Id.* at 33.

165. *Id.* at 33–34.

166. *Carpenter*, 138 S. Ct. at 2220.

167. 45 C.F.R. § 164.512(f)(1)(ii) (2018) (permitting disclosure of protected health information pursuant to a court order or grand jury subpoena).

168. See Ohm, *Sensitive Information*, *supra* note 87, at 1150–53.

sub-factors probably weigh about the same for these records as for CSLI: most medical providers keep records dating back to the beginning of their interaction with a patient and it would cost the police an exorbitant sum to compile the kind of information it can access for very little.

The other subfactors and factors cut the other way. The main sub-factor that distinguishes CSLI from medical records is depth. The metronomic regularity with which an individual's location is tracked seemed quite important to the majority opinion.¹⁶⁹ In contrast, most people interact with the health care system only on occasion.¹⁷⁰

Finally, while the creation of medical records might be as inescapable as CSLI, they usually are not as automatic. Unlike the take-it-or-leave-it and invisible quality of CSLI gathering, most medical records are populated in clearly delineated interactions, when we are aware that we are literally being poked, prodded, and measured.

For these reasons, lower courts will likely consider medical record data to be a relatively close call. For ordinary healthy individuals, their medical records — while undoubtedly sensitive — are not nearly the product of the same kind of “tireless and absolute surveillance” at issue in *Carpenter*.¹⁷¹ The digitization of these records has not experienced the same dramatic gains in efficiency as the tracking of location or reading habits.

What about a copy of an individual's DNA stored with a private third party? In his dissent, Justice Gorsuch opines without analysis that “most lawyers and judges today” would require a warrant and probable cause to access DNA voluntarily stored with 23andMe.¹⁷² This provides an important window into Justice Gorsuch's baseline attitude about the Fourth Amendment and might also offer a window into how to directly appeal to him in the future. But this conclusion certainly doesn't flow from the *Carpenter* factors.

Without a doubt, a copy of an individual's genome satisfies the deeply revealing nature factor. Genetic information reveals propensity for disease, physical and mental characteristics, parentage, and genealogy.¹⁷³ It reveals this not only for the individual who uploaded the DNA but also for close relatives.¹⁷⁴

169. See *Carpenter*, 138 S. Ct. at 2218.

170. The exceptions are hospitalized patients and people diagnosed with chronic or terminal conditions. Many of these people might be connected to 24/7 electronic devices that generate information in exactly the same fashion as a smart phone.

171. *Id.*

172. *Id.* at 2262 (Gorsuch, J., dissenting).

173. Mike Silvestri, Note, *Naturally Shed DNA: The Fourth Amendment Implications in the Trail of Intimate Information We All Cannot Help But Leave Behind*, 41 U. BALT. L. REV. 165, 168 (2011).

174. Erin Murphy, *Relative Doubt: Familial Searches of DNA Databases*, 109 MICH. L. REV. 291, 313 (2010).

None of the other factors seem to trigger the same concerns as CSLI. A single copy of the three billion base pairs that comprise a human DNA does not track activity and change over time, unlike most of the other examples we have considered. At least under 23andMe's current business model, submissions are fundamentally voluntary, although individuals who did not submit their DNA will be able to argue about the inescapable nature of their presence in close relatives' genetic data if the police target them through their relatives' submissions.¹⁷⁵

It seems unlikely that a court would require a warrant for DNA evidence held by a private third party based on a straight application of the *Carpenter* factors. This is not to say that there might not be other applications of the REP test that would protect this information. It is a reminder that *Carpenter* is not the only path to finding that a Fourth Amendment search has occurred.

The basic rule of *Carpenter* alone presents a fundamental change to Fourth Amendment doctrine. It requires a warrant in many situations where none were required before. But this important change is just the first of many found within the reasoning of this opinion.

III. BEYOND THE CORE TEST OF *CARPENTER*

Based on the new substantive rule it announces, *Carpenter* is already on par with some of the most consequential Fourth Amendment cases of all time. But when you look beyond the core rule to some of the other revolutions wrought in the opinion, it is possible to conclude that *Carpenter* represents a fundamental shift, not merely an incremental adaptation. It turns the third-party doctrine inside out, requiring the government to account for the database design and information-gathering decisions of private parties, decisions made without any state intervention. Its broad reasoning will apply not only when third parties are involved but also when the government conducts detailed digital surveillance by itself. It also creates three new rules of technological equivalence, which are much more straightforward to apply than the multi-factor test and therefore, might end up being applied more often than the core rule itself.

A. *Carpenter* as a Replacement for *Katz*

The conventional wisdom suggests that *Carpenter* is an application or expansion of the *Katz* REP test. We might think of it instead as an outright replacement for REP, at least for cases involving complex modern technology.

175. *Id.* at 297–301, 337 (explaining the mechanics behind familial searches through DNA databases in criminal cases).

Carpenter settles long-standing disputes about both prongs of the *Katz* test. It affirms the conclusion that “*Katz* Has Only One Step”¹⁷⁶ by providing no analysis whatsoever into the defendant’s subjective expectation of privacy. For the objective prong, *Carpenter* means that the Court has at long last answered the fundamental question about REP: does the objective prong merely describe the expectations of ordinary Americans or does it ask judges to propound a normative vision for the kind of society the Constitution seeks to protect? *Carpenter* selects the normative over the descriptive: the role of courts is to protect the balance of power between the state (in the form of the police) and the people, refusing to let technological change eviscerate individual privacy and security from the state.¹⁷⁷

These changes do more than apply or extend *Katz*. They reinvent and supplant that venerable opinion. The REP test has been replaced by *Carpenter*’s multi-factor test and the rule of technological equivalence. Time will reveal that the *Katz* era has ended. This is a welcome development; the *Carpenter* era will be seen as more predictable, constitutionally supported, and responsive to the rate of technological change than the REP test it has replaced.

1. The Subjective Prong: *Katz* Has Only One Step

Carpenter supports what Orin Kerr has argued: “the subjective prong [of the REP test] has become a phantom doctrine.”¹⁷⁸ As initially expressed in Justice Harlan’s concurrence, the REP test was a two-pronged inquiry: “first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as ‘reasonable.’”¹⁷⁹

Scholars have offered at least three different interpretations for the subjective prong, none of which appear in *Carpenter*. Most often, courts seem to treat the subjective test as an inquiry into what the person actually intended in her mind.¹⁸⁰ Did this person actually believe her actions or communications were shielded from public view? The problem with this formulation is that it never seems to matter. Almost never is a court confronted with a situation in which this version of the subjective prong fails but the objective prong does not.¹⁸¹

176. See generally Orin S. Kerr, *Katz Has Only One Step: The Irrelevance of Subjective Expectations*, 82 U. CHI. L. REV. 113, 113 (2015) [hereinafter Kerr, *One Step*].

177. *Carpenter*, 138 S. Ct. at 2246.

178. Kerr, *One Step*, *supra* note 176, at 133.

179. *Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

180. Kerr, *One Step*, *supra* note 176, at 130–31.

181. See *id.* at 116–22 (examining all published opinions analyzing the Fourth Amendment reasonable expectation of privacy test in 2012 and finding that not a single case “relied on the subjective test in an outcome-determinative way”).

Kerr argues that the subjective prong could instead have been read, long ago, to place more emphasis on Justice Harlan's use of the word "exhibited."¹⁸² By this reading, the subjective prong asks whether the defendant had "voluntarily exposed" information to the public. Critically, this version of the test would not require courts to probe the inner mind of the person asserting privacy. Rather, it would look to the objective measures the person took to block the government's view.¹⁸³

A third way of interpreting the subjective prong is offered by Lior Strahilevitz and Matthew Kugler.¹⁸⁴ They argue that courts should consult survey evidence in the subjective prong, "us[ing] the sentiments of the median American citizen as a proxy for the defendant's subjective expectation of privacy."¹⁸⁵

We do not know how the *Carpenter* court interpreted the subjective prong because the majority's opinion gives it almost no attention. The opinion never mentions the word "subjective." Its recitation of the REP test barely nods at this as a separate requirement: An REP is "[w]hen an individual 'seeks to preserve something as private,' and his expectation of privacy is 'one that society is prepared to recognize as reasonable'"¹⁸⁶ In applying the test, the Court makes no attempt to analyze subjective and objective expectations separately.

Carpenter did not put a nail in the coffin of the subjective prong, because it was interred long ago.¹⁸⁷ The subjective prong has become an unmarked grave, one courts trample from above, not even acknowledging the presence of the decomposed remains underfoot.

2. The Objective Prong: Victory of the Normative Fourth Amendment

By recognizing tech exceptionalism, the *Carpenter* court restores — at least for the time being — the normative vision of the Fourth Amendment, taking sides in a very old debate: is the objective prong of the REP test — which asks, is society prepared to accept an expectation of privacy as reasonable — a descriptive or normative inquiry?¹⁸⁸ Is it the judge's role to examine what the reasonable individual or median member of society expects, or is it the judge's charge to

182. *Id.* at 127.

183. *Id.* at 126.

184. Matthew B. Kugler & Lior Jacob Strahilevitz, *Actual Expectations of Privacy, Fourth Amendment Doctrine, and the Mosaic Theory*, 2015 SUP. CT. REV. 205, 240–44 (2015) [hereinafter Kugler & Strahilevitz, *Actual Expectations*].

185. *Id.* at 241.

186. *Carpenter v. United States*, 138 S. Ct. 2206, 2213 (2018).

187. Kerr, *One Step*, *supra* note 176, at 114 (attributing abandonment of subjective prong to cases from the 1970s and 1980s).

188. Anthony G. Amsterdam, *Perspectives on the Fourth Amendment*, 58 MINN. L. REV. 349, 382–84, 391–93, 404 (1974).

imagine how the court's rulings can help set our society onto a particular path?¹⁸⁹

Justice Harlan, who first conceived of the REP test, made his opinion about this question quite clear only four years after *Katz*, albeit in dissent:

Since it is the task of the law to form and project, as well as mirror and reflect, we should not, as judges, merely recite the expectations and risks without examining the desirability of saddling them upon society. The critical question, therefore, is whether under our system of government, as reflected in the Constitution, we should impose on our citizens the risks of the electronic listener or observer without at least the protection of a warrant requirement.¹⁹⁰

Too often, the Court has strayed from this path, thinking of its role in interpreting REP as merely descriptive.¹⁹¹

Carpenter advances the idea that, at least when police surveillance technology changes rapidly, the proper role for the court is the normative one Justice Harlan advocated. We should not saddle society with merely what it has come to expect.¹⁹²

Tech exceptionalism once again settles this question. The proper accounting of the way technology has disrupted individual privacy, distorted society, and rebalanced the power between the state and its citizens thrusts the judiciary into a more aggressive role in interpreting the Fourth Amendment than it has assumed in the past.

This, once again, is at the heart of Orin Kerr's equilibrium adjustment theory and Bankston and Soltani's theory of government efficiency gain.¹⁹³ The Constitution is premised on an ordinary rate of change in the balance of power between the state and the people. The Fourth Amendment is our national thermostat, recalibrating what the

189. Kerr, *Four Models*, *supra* note 89, at 507–24.

190. *United States v. White*, 401 U.S. 745, 786 (1971) (Harlan, J., dissenting).

191. *See, e.g., Bond v. United States*, 529 U.S. 334, 338 (2000) (“When a bus passenger places a bag in an overhead bin, he expects that other passengers or bus employees may move it for one reason or another. Thus, a bus passenger clearly expects that his bag may be handled.”); *California v. Ciraolo*, 476 U.S. 207, 215 (1986) (“In an age where private and commercial flight in the public airways is routine, it is unreasonable for respondent to expect that his marijuana plants were constitutionally protected from being observed with the naked eye from an altitude of 1,000 feet.”); *Smith v. Maryland*, 442 U.S. 735, 744 (1979) (“When he used his phone, petitioner voluntarily conveyed numerical information to the telephone company and ‘exposed’ that information to its equipment in the ordinary course of business. In so doing, petitioner assumed the risk that the company would reveal to police the numbers he dialed.”).

192. *Cf. Kerr, Four Models*, *supra* note 89, at 543–44.

193. Bankston and Soltani, *supra* note 70, at 335–38; Kerr, *Equilibrium-Adjustment*, *supra* note 73, at 84.

police can and cannot do. In periods of ordinary change for policing technology — which I believe describes the first two hundred years or so of our national experience — we could afford a merely descriptive Fourth Amendment, assigning to the courts a relatively passive role in mediating the relationship between state power and the people. But when faced with the disruptive technological restructuring of power and institutions, the normative Fourth Amendment — and the court's central role in protecting and strengthening it — becomes an imperative.

3. The Argument for Moving Beyond *Katz*

Once we recognize that *Carpenter* has moved beyond *Katz* in important ways, we should ask whether this is a desirable result. I contend that the future sketched out by *Carpenter* is preferable to the world *Katz* has given us.

First, *Carpenter*'s multi-factor test will lead to more predictability than *Katz*'s. The REP test has always been open-textured and ambiguous. What is a reasonable expectation of privacy? Is the objective prong to be analyzed descriptively or normatively?

Ambiguous at birth, the subsequent decades have done very little to lend *Katz* concreteness or predictability. Orin Kerr persuasively argues that the Court chooses from a menu of four different approaches — private facts, probabilistic, positive law, and policy — to assess REP.¹⁹⁴ But it is hard to discern a pattern to when the Court chooses each.¹⁹⁵

In contrast, the multi-factor test is relatively easy to apply. There will likely be disagreement about how to apply, say, the “depth, breadth, and comprehensive reach” factor to different databases.¹⁹⁶ But the spectrum of disagreement will be narrow and cabined compared to the wide ranging across Kerr's four models that *Katz* has created.¹⁹⁷ *Carpenter* sweeps away the cacophony of the four models, selecting a normative-over-descriptive methodology with three concrete factors.

Second, the approach is, if anything, more closely connected to the text and history of the Constitution. To be clear, neither *Katz* nor *Carpenter* purports to adhere closely to the text and history. But *Katz* suffered by focusing on a principle — privacy — that is nowhere to be seen in the literal text of the amendment.

194. Kerr, *Four Models*, *supra* note 89, at 506.

195. *Id.* at 524 (“The hard cases tend to be those in which the different models point judges to different conclusions. In those cases, courts must choose which model applies to that particular case.”).

196. See *supra* Section II.C.2 (discussing difficulty of the line-drawing inherent in these factors).

197. *Id.*

In contrast, *Carpenter*'s test and reasoning resonate much more directly with history. The Court primarily treats the Fourth Amendment as a restriction on government power, not just a protection of privacy.¹⁹⁸ The factors hone in on the features of data that fuel the government's power. "Comprehensive reach" allows the government to conduct surveillance on the entire populace; "breadth" allows it to peer back in time; "depth" and "deeply revealing nature" raise the prospect of meaningful harm.¹⁹⁹

In addition, the location information in *Carpenter* and the smart phone in *Riley* are arguably intrinsic aspects of individual personality, connecting them to the "persons" recited in the text of the Fourth Amendment.²⁰⁰

Third, the tech exceptionalism at the heart of the new test impels courts to engage in a deep consideration of the specific features of technology and society's embrace of technology that was usually lacking from the conventional REP test. This will prevent the kind of inadequate responsiveness to progress that plagued the third-party doctrine from its birth.

B. The Third-Party Doctrine, Inside Out

Carpenter concludes that location information is protected "[w]hether the Government employs its own surveillance technology as in *Jones* or leverages the technology of a wireless carrier"²⁰¹ This quote is breathtaking. It calls into question the bedrock rule that the Fourth Amendment concerns itself only with the activities of the government.²⁰² The police have never before had to account so fully for the independent decisions or actions of private actors. A private citizen could literally break into a house, break into a safe inside the house, steal what lay within the safe, and deliver the contents of the safe to the police.²⁰³ So long as the police had nothing to do with the thief before

198. *Carpenter v. United States*, 138 S. Ct. 2206, 2214 (2018) ("[T]he Amendment seeks to secure 'the privacies of life' against 'arbitrary power' [A] central aim of the Framers was 'to place obstacles in the way of a too permeating police surveillance.'").

199. *Supra* Section II.C.2.

200. U.S. CONST. amend. IV.

201. *Carpenter*, 138 S. Ct. at 2217.

202. *United States v. Jacobsen*, 466 U.S. 109, 113 (1984) ("This Court has also consistently construed this protection as proscribing only governmental action; it is wholly inapplicable to a search or seizure, even an unreasonable one, effected by a private individual not acting as an agent of the Government or with the participation or knowledge of any governmental official.").

203. *See United States v. Jarrett*, 338 F.3d 339, 347–48 (2006) (holding that receiving evidence from an anonymous hacker who had taken files from defendant's computer did not constitute government action and thus did not violate the Fourth Amendment).

he arrived at the stationhouse, they would be free to use the contents in court.²⁰⁴

For the first time, even though the police are not responsible for the decisions that led to the collection of potential evidence, they nevertheless are held to account for the nature of the information collected. This has blurred the government action requirement in some important ways.

Of the three *Carpenter* factors, the one that is most influenced by the choices made by private actors is “depth, breadth, and comprehensive reach.”²⁰⁵ To be clear, the Court does not seem to be delving into the motivations of cell phone providers; warrant suppression hearings will not turn on the testimony of a T-Mobile executive explaining why the company structures its data the way it does. But the constitutional meaning of the word “search” in cases like these now turns intrinsically on the results of the business decisions of companies.

Consider the breadth factor. The majority opinion emphasizes the importance of the “time machine” quality of CSLI. “With access to CSLI, the Government can now travel back in time to retrace a person’s whereabouts, subject only to the retention policies of the wireless carriers, which currently maintains records for up to five years.”²⁰⁶ For the most part, at least in the United States, corporate retention policies are not set by regulation.²⁰⁷ Each company must weigh the potential benefits of having access to old data against the cost of data storage and the potential trouble in the form of cybersecurity risk or regulatory scrutiny. Practices vary widely even between companies in the same industry.²⁰⁸ These choices are not made in consultation with the police, yet *Carpenter* has now given these private decisions constitutional weight.²⁰⁹

204. *See id.*

205. *Carpenter*, 138 S. Ct. at 2223.

206. *Id.* at 2218.

207. *See* Catherine Crump, Note, *Data Retention: Privacy, Anonymity, and Accountability Online*, 56 STAN. L. REV. 191, 193 (2003) (discussing the role of “data preservation” in the United States, in the absence of a data retention mandate). One rare exception is that the FCC requires telephone companies to keep billing information about telephone toll calls for eighteen months. 47 C.F.R. § 42.6 (2019). In 2006, the European Union enacted a Data Retention Directive that mandated providers of some communications services to retain certain data for six to twenty-four months. Council Directive 2006/24, art. 1, 2006 O.J. (L 105) 54 (EC). It was declared invalid by the Court of Justice of the European Union in 2014. Joined Cases C-293/12 & C-594/12, *Digital Rights Ir. Ltd. v. Ireland* (Apr. 8, 2014), <http://curia.europa.eu/juris/document/document.jsf?text=&docid=162437&pageIndex=0&doclang=en&mode=req&dir=&occ=first&part=1&cid=1539063> [https://perma.cc/PPQ9-LD6C].

208. Ernesto Van der Sar, *How Long Does Your ISP Store IP-Address Logs?*, TORRENT-FREAK (June 29, 2012), <https://torrentfreak.com/how-long-does-your-isp-store-ip-address-logs-120629> [https://perma.cc/SNR4-QEV4] (reporting IP address retention policies by ISPs from two weeks to eighteen months).

209. *Carpenter*, 138 S. Ct. at 2218 (focusing on importance of fact that CSLI is stored for five years).

The same can be said for the depth factor. Every company decides how much information to track and retain. Returning again to web-browsing surveillance, some ISPs retain very little evidence of the web browsing habits of their customers; others deploy deep packet inspection to view and store information about the content of communications between individuals and websites.²¹⁰ The first time the government is forced to defend against a challenge to the warrantless access to this kind of information, its fate might turn on where the ISP chose to position itself along this spectrum.

It could be argued, then, that the Court did more than narrow the third-party doctrine; it turned the third-party doctrine inside out. Not only does the mere fact that a target trusted personal information with a third party no longer insulate that data from Fourth Amendment scrutiny, the constitutional duties imposed on the police might also now turn on the independent decisions of third parties.

C. Carpenter and Direct Government Surveillance

Carpenter's reasoning should apply even when third parties are not involved. Its multi-factor test focuses most of its attention on the quality of the database alone, so it should apply even to databases compiled directly by the government. It might apply, for example, to analyze the use by the police of suspicionless, automated data collection techniques such as drone monitoring or facial recognition techniques used on surveillance camera data.²¹¹

Consider automated license plate readers ("ALPRs").²¹² These devices contain stationary cameras that sit for days, weeks, or longer on the side of the road, deployed by government officials for the express purpose of recording the license plate numbers of cars that pass by a particular location.²¹³ These records are fed into databases from which the police can search for particular vehicles and that are sometimes automatically searched to locate stolen or unregistered cars, kidnap victims, or missing persons.²¹⁴

A simplistic view of *Carpenter* would assume it had nothing to say about ALPRs. Because this technology does not involve private parties

210. Ohm, *Invasive ISP Surveillance*, *supra* note 9, at 1432–37.

211. GARVIE ET AL., *supra* note 60, at 31–33.

212. Rachel Levinson-Waldman, *Hiding in Plain Sight: A Fourth Amendment Framework for Analyzing Government Surveillance in Public*, 66 EMORY L.J. 527, 544–46 (2017). See generally Randy L. Dryer & S. Shane Stroud, *Automatic License Plate Readers: An Effective Law Enforcement Tool or Big Brother's Latest Instrument of Mass Surveillance? Some Suggestions for Legislative Action*, 55 JURIMETRICS J. 225 (2015); Jessica Gutierrez Alm, Note, *The Privacies of Life: Automatic License Plate Recognition is Unconstitutional Under the Mosaic Theory of Fourth Amendment Privacy Law*, 38 HAMLINE L. REV. 127 (2015).

213. Dryer & Stroud, *supra* note 212, at 229–32.

214. Kimberly J. Winbush, *Use of License Plate Readers*, 32 A.L.R. 7TH ART. 8 (2017).

doing the data collection, this falls out of the potential application of the third-party doctrine.²¹⁵ Ignoring *Carpenter*, this case might be seen as a fairly straightforward application of Fourth Amendment cases involving plain view, knowing exposure, and reduced expectations of privacy in automobiles.²¹⁶ This simplistic view would suggest that no justification or judicial review is required to collect information with an ALPR — much less a search warrant.²¹⁷

The better reading is to understand that *Carpenter* has rewritten the rules for assessing the reasonable expectation of privacy in massive data gathering efforts, whether or not they are instigated by private actors.

How, then, does ALPR fare under the *Carpenter* factors? Because ALPR gives the police the ability to track the location and movement of cars, it seems superficially similar to CSLI. But because ALPR measures location only at fixed points throughout a city, it is likely to be seen as less problematic than CSLI for many of the *Carpenter* factors.²¹⁸ ALPR generates data that is neither as deep, broad, nor comprehensive as CSLI.²¹⁹ Because there is less data, it collectively is less deeply revealing than CSLI.²²⁰ For those who drive, ALPR is as inescapable and automatic as CSLI, but the same is not true for those with smartphones but not cars.

In the end, courts must balance these factors and determine whether ALPR implicates privacy enough to qualify as an invasion of a reasonable expectation of privacy. It is likely to be a very close call. But nothing in *Carpenter*'s reasoning or multi-factor test suggests that they apply only when third parties are involved.

215. To be clear, some ALPR implementations are run by private companies, who sell the data collected to state entities. See Justin Rolich, *In Just Two Years, 9,000 of these Cameras Were Installed to Spy on Your Car*, QUARTZ (Feb. 5, 2019), <https://qz.com/1540488/in-just-two-years-9000-of-these-cameras-were-installed-to-spy-on-your-car> [https://perma.cc/6VC4-5H2G] (describing spread of ALPR technology to private companies and the general public).

216. *New York v. Class*, 475 U.S. 106, 114 (1986) (holding no reasonable expectation of privacy in automobile's vehicle identification number); *Cardwell v. Lewis*, 417 U.S. 583, 590 (1974) (plurality opinion) ("One has a lesser expectation of privacy in a motor vehicle . . .").

217. *United States v. Yang*, No. 2:16-cr-231-RFB, 2018 WL 576827 at *6 (D. Nev. Jan. 25, 2018) (holding no reasonable expectation of privacy in data collected in commercial license plate location database).

218. Alm, *supra* note 212, at 151–52 (conceding that ALPR data is more intermittent and thus less sensitive than GPS data collected over the same period of time).

219. *Id.* See *Yang*, 2018 WL 576827, at *6 (distinguishing *Jones* because ALPR does not "provide[] continuous contemporaneous information about the location of a vehicle" and does not "create[] a travel history of all of the movements of the targeted vehicle").

220. Alm, *supra* note 212, at 151–52.

D. The New Rule of Technological Equivalence

Up to this point, I have focused almost entirely on the rules deriving from the majority opinion signed by five justices. Even more can be surmised by what the dissents added, because even though they disagreed with the majority's holding and reasoning, they provide tantalizing concessions suggesting that they too are willing to read the Fourth Amendment to cover more police conduct than the Court has recognized in the past. One must be careful not to read too much into dissents, naturally. I am placing stock in arguments made by Justices Gorsuch and Kennedy, who might have been making rhetorical points rather than hinting at their future votes.²²¹

With those caveats in mind, reading all of the Carpenter opinions together suggests a broad new rule of technological equivalence. Any police activity that is the modern-day equivalent of activity that has been long protected under the Fourth Amendment is now protected.²²²

The new test relies on a simple syllogism: the Court in the past has held that information in a particular, traditional privacy context is protected by the Fourth Amendment. A technology produces information that is a modern-day equivalent of the information produced in that traditional context. The information in the modern context is also protected by the Fourth Amendment.

There are three major strands of this new test in these opinions: activity that is technologically equivalent to prying into (1) the intimacy of the home, (2) into papers held in bailment, and (3) into private communications. Consider each in turn.

1. Information from Inside the Home

The rule of technological equivalence springs from *Kyllo*, the 2001 case involving police use of a thermal imaging device pointed at a suburban home in Florence, Oregon.²²³ To prove that the defendant was growing marijuana inside his home, they used the device to reveal the heat that emanated from powerful grow lights and compared it to the ordinary heat patterns of his neighbors.²²⁴ The Supreme Court, in an opinion by Justice Scalia, held that using a thermal imager on a home constituted a Fourth Amendment search.²²⁵

221. Justice Kennedy, of course, will not cast any future votes!

222. *Carpenter v. United States*, 138 S. Ct. 2206, 2230 (2018) (Kennedy, J., dissenting).

223. *Kyllo v. United States*, 533 U.S. 27, 29 (2001).

224. *Id.* at 29–30.

225. *Id.* at 34–35.

Carpenter cites two crucial propositions from *Kyllo*.²²⁶ The first is the idea that an inference can be a search.²²⁷ The second is the proposition that when courts assess the impact of rapidly changing technology under the Fourth Amendment, they look not only at the technology used in the facts of the case, but they also extrapolate to future, more powerful versions of the technology. “While the technology used in the present case was relatively crude, the rule we adopt must take account of more sophisticated systems that are already in use or in development.”²²⁸

Putting these together, the first rule of technological equivalence applies to any information that reveals details from inside the home. The centerpiece of Justice Scalia’s reasoning in *Kyllo* was that “in the home . . . all details are intimate details.”²²⁹ This kind of reasoning is quite likely to extend Fourth Amendment protection to the information generated by many devices that comprise the Internet of Things, because so much of it focuses on the interior of the home.²³⁰ Smart speakers such as the Amazon Echo and Google Home record sounds from the inside of a home.²³¹ Smart TVs record the entertainment consumed in a home.²³² The Nest thermostat records the temperature of the home.²³³ And the Ring doorbell records visitors to the home.²³⁴ The police can obtain records like these as evidence in criminal investigations.²³⁵

226. *Carpenter*, 138 S. Ct. at 2218–19.

227. *Kyllo*, 533 U.S. at 36; *id.* at 44 (Stevens, J., dissenting) (criticizing the majority: “For the first time in its history, the Court assumes that an inference can amount to a Fourth Amendment violation”).

228. *Id.* at 36.

229. *Id.* at 37.

230. See Andrew Guthrie Ferguson, *The Internet of Things and the Fourth Amendment of Effects*, 104 CALIF. L. REV. 805, 836–42 (2016).

231. Michael Harrigan, *Privacy Versus Justice: Amazon’s First Amendment Battle in the Cloud*, 45 W. ST. L. REV. 91, 91–93 (2017) (discussing government’s attempt to obtain Amazon Echo recording for a murder trial); Arielle M. Rediger, *Always-Listening Technologies: Who Is Listening and What Can Be Done About It*, 29 LOY. CONSUMER L. REV. 229, 231, 239–40 (2017) (discussing privacy implications of Amazon Echo and Google Home).

232. Whitson Gordon, *How to Stop Your Smart TV from Tracking What You Watch*, N.Y. TIMES (July 23, 2018), <https://www.nytimes.com/2018/07/23/smarter-living/how-to-stop-your-smart-tv-from-tracking-what-you-watch.html> [<https://perma.cc/78UB-4G27>].

233. Jillisa Bronfman, *Weathering the Nest: Privacy Implications of Home Monitoring for the Aging American Population*, 14 DUKE L. & TECH. REV. 192, 196–99 (2016) (discussing privacy implications of Nest Labs products); David C. Vladeck, *Consumer Protection in an Era of Big Data Analytics*, 42 OHIO N.U. L. REV. 493, 511 (2016) (discussing privacy implications of Google Nest and competitors).

234. Reed Albergotti, *How Amazon’s Latest Security Device Let People Spy on You*, THE INFORMATION (May 11, 2018, 7:01 AM), <https://www.theinformation.com/articles/how-amazons-latest-security-device-let-people-spy-on-you> [<https://perma.cc/E3RF-RC8N>] (discussing privacy vulnerability of Ring doorbell system).

235. James O’Toole, *Cops can access your connected home data*, CNN (June 16, 2014, 2:25 PM), <https://money.cnn.com/2014/06/16/technology/smart-home-footage/index.html> [<https://perma.cc/TJ3G-9KPS>] (discussing tech companies’ requirements to release home security footage to law enforcement).

The *rule of equivalence to the home* suggests that the police now need a warrant to obtain any of this information.²³⁶ The *Kyllo* reasoning suggests that we need not even consider the sensitivity or intimacy of the information obtained, because “all details are intimate details.”²³⁷

Notice that the technological equivalence rule is far simpler and more predictable to apply than the majority’s multi-factor test. Once the equivalence is made, the conduct is ruled a search, and the analysis ends. One need not endure the multi-factor gymnastics required to analyze the status of CSLI.

Just a few months after *Carpenter* was decided, the Seventh Circuit applied this rule. In *Naperville Smart Meter Awareness v. Naperville*,²³⁸ the court held that a city’s mandatory use of smart meters on homes constituted a search under the Fourth Amendment.²³⁹ Because different appliances produce different “load signatures,” “researchers can predict the appliances that are present in a home and when those appliances are used.”²⁴⁰ This “reveals when people are home, when people are away, when people sleep and eat, what types of appliances are in the home, and when those appliances are used.”²⁴¹ Although the case cites *Carpenter* in a brief passage declining to apply the third-party doctrine, its core reasoning is an application of *Kyllo*.²⁴²

2. Bailment

Both Justices Kennedy and Gorsuch lean on the law of bailment, suggesting a revitalization of this ancient legal concept by prosecutors and criminal defense lawyers. Consider Justice Gorsuch’s academic disquisition on the idea:

[T]he fact that a third party has access to or possession of your papers and effects does not necessarily eliminate your interest in them. Ever hand a private document to a friend to be returned? Toss your keys to a valet at a restaurant? Ask your neighbor to look after your dog while you travel? You would not expect the

236. See, e.g., Zack Whittaker, *Judge Orders Amazon to Turn Over Echo Recordings in Double Murder Case*, TECHCRUNCH (Nov. 14, 2018), <https://techcrunch.com/2018/11/14/amazon-echo-recordings-judge-murder-case> [<https://perma.cc/E6A2-SVNL>] (reporting a New Hampshire court’s grant of a police search warrant to access Amazon Echo recordings in a double murder case).

237. *Kyllo v. United States*, 533 U.S. 27, 37 (2001).

238. 900 F.3d 521 (7th Cir. 2018).

239. The court ruled that the search was reasonable because the smart meter information was gathered for a non-criminal-investigation government purpose, and the benefits of the program outweighed the intrusion on privacy. *Id.* at 527–29.

240. *Id.* at 524.

241. *Id.* at 526.

242. *Id.*

friend to share the document with others; the valet to lend your car to his buddy; or the neighbor to put Fido up for adoption. Entrusting your stuff to others is a *bailment*. A bailment is the “delivery of personal property by one person (the *bailor*) to another (the *bailee*) who holds the property for a certain purpose.” Black’s Law Dictionary 169 (10th ed. 2014) A bailee normally owes a legal duty to keep the item safe, according to the terms of the parties’ contract if they have one, and according to the “implication[s] from their conduct” if they don’t. 8 C. J. S., Bailments § 36, pp. 468-469 (2017). A bailee who uses the item in a different way than he’s supposed to, or against the bailor’s instructions, is liable for conversion. *Id.*, § 43, at 481 These ancient principles may help us address modern data cases too. Just because you entrust your data—in some cases, your modern-day papers and effects—to a third party may not mean you lose any *Fourth Amendment* interest in its contents. Whatever may be left of *Smith* and *Miller*, few doubt that e-mail should be treated much like the traditional mail it has largely supplanted—as a bailment in which the owner retains a vital and protected legal interest.²⁴³

Justice Kennedy, while not engaging with the idea at such length, seems to agree that modern-day equivalents to bailment ought not to be subject to the third-party doctrine.²⁴⁴

This reasoning, by two justices in dissent,²⁴⁵ signals quite clearly that the Court will someday rule that “modern-day papers and effects” held by third parties will be protected by the Fourth Amendment. This seems to describe almost perfectly the contemporary state of cloud computing. Services like Google Drive and Dropbox allow individuals to move their modern-day papers into the cloud.²⁴⁶ Services like Amazon Web Services create dedicated virtualized computers on cloud

243. *Carpenter v. United States*, 138 S. Ct. 2206, 2268–69 (2018) (Gorsuch, J., dissenting).

244. *Id.* at 2228 (Kennedy, J., dissenting) (noting that the private parties in *Smith* and *Miller* “were not bailees or custodians of the records” at issue); see also *id.* at 2259 n.6 (Alito, J., dissenting) (“[T]his is not a case in which someone has entrusted papers that he or she owns to the safekeeping of another, and it does not involve a bailment.”).

245. Four, if you include Justices Alito and Thomas, who signed Justice Kennedy’s dissent.

246. Mickey Meece, *A User’s Guide to Finding Storage Space in the Cloud*, N.Y. TIMES, (May 16, 2012), <https://www.nytimes.com/2012/05/17/technology/personaltech/a-computer-users-guide-to-cloud-storage.html> (last visited May 11, 2019); *What is Dropbox*, DROPBOX, <https://www.dropbox.com/features> [<https://perma.cc/23WP-MAFW>]; *Google Drive*, GOOGLE, <https://gsuite.google.com/products/drive/> [<https://perma.cc/FU2V-ZRXC>].

servers, which customers can fill with data, which other users are not permitted to access.²⁴⁷ If law enforcement tries to obtain any information stored on services such as these, it seems quite likely that lower courts will rule such accesses to be controlled by the *technological equivalence of bailment* rule, thus requiring a warrant.

3. Private Communications

Similarly, all nine justices signed onto opinions that declare that the police need a warrant to read the content of email messages.²⁴⁸ Although this is still dicta, it is stated clearly enough so that lower courts can and should begin to rely on the clear signal.

This is important because, to date, only one appellate court, the Sixth Circuit, has required the police to obtain a warrant to access the content of stored email messages, in the 2010 case *United States v. Warshak*.²⁴⁹ *Warshak* itself is cited approvingly in *Carpenter* in three separate opinions: the majority,²⁵⁰ and the dissents by Justices Kennedy,²⁵¹ and Gorsuch.²⁵²

This is yet another application of the rule of technological equivalence: the *rule of equivalence to private communications*. In the 1877 case of *Ex Parte Jackson*, the Court required a warrant to open sealed letters in the possession of the postal service.²⁵³ Emails, “the technological scion of tangible mail,” according to the *Warshak* court,²⁵⁴ are the modern equivalents of postal letters from the time of *Ex Parte Jackson*.

As noted above, all nine justices have now signaled they would hold that the contents of email are protected by the Fourth Amendment. The police must obtain a search warrant, or proceed under an exception to the warrant requirement such as exigent circumstances, to access the contents of email messages.²⁵⁵

It is likely that this rule will protect other forms of electronic communications other than email. Any person-to-person communications

247. Alex Hern, *Amazon Web Services: The secret to the online retailer's future success*, THE GUARDIAN, (Feb. 2, 2017, 2:00 AM), <https://www.theguardian.com/technology/2017/feb/02/amazon-web-services-the-secret-to-the-online-retailers-future-success> [https://perma.cc/4Y33-AVFR]; *What is AWS?*, AMAZON WEB SERVS., <https://aws.amazon.com/what-is-aws> [https://perma.cc/KYN9-Y5QR].

248. *Carpenter*, 138 S. Ct. at 2222; *id.* at 2230 (Kennedy, J., dissenting); *id.* at 2269 (Gorsuch, J., dissenting).

249. 631 F.3d 266, 288 (6th Cir. 2010).

250. *Carpenter*, 138 S. Ct. at 2222.

251. *Id.* at 2230.

252. *Id.* at 2269.

253. 96 U.S. 727, 733 (1877) (requiring a warrant to open sealed letters in the possession of the postal service).

254. 631 F.3d at 286.

255. *Id.* at 288.

are likely protected. The police most likely now need a warrant to obtain, from storage or in real-time, instant messages, direct messages on a social networking service, or text messages.²⁵⁶

Carpenter upends Fourth Amendment doctrine. Its most revolutionary contribution, however, might be what it has done to Fourth Amendment reasoning.

IV. CARPENTER'S TECH EXCEPTIONALISM

The beating heart of the *Carpenter* majority opinion is its deep and abiding belief in the exceptional nature of the modern technological era. This seems to come directly from Chief Justice Roberts, who revealed the same attitude four years earlier in the majority opinion in *Riley v. California*.²⁵⁷ Recent advances in technology such as the smartphone and the Internet have led to differences in kind and not merely in degree from the technology of the past.

The Chief Justice's break with the technological past supports a break with judicial precedent in several ways. A belief in the exceptionalism of modern technology leads one to dismiss otherwise conventional analogies. *Riley* and *Carpenter* both refuse to compare smartphones to past technologies, such as address books, diaries, or even telephones.²⁵⁸ Because analogical reasoning sits at the heart of legal reasoning and stare decisis, the Court's rejection of analogies like these gives it an opening to chart a new path.

Reasoning about exceptional technology requires courts to develop a deep understanding of technology, and these opinions are notable for the way they rely heavily on technological explication. They are full of citations to amici briefs and they press the boundaries of judicial notice.

Finally, the Court's adoption of tech exceptionalism closes the door on scholars who have been trying to reinvent *Katz* by appealing to surveys, history, or positive law. Each of these three approaches peers into our past and relies on the ability of lay people to understand what has changed. *Carpenter* and *Riley* instead look into the future, and for that reason, reject all three of these proposals.

256. Compare Michael W. Price, *Rethinking Privacy: Fourth Amendment Papers and the Third-Party Doctrine*, 8 J. NAT'L SEC. L. & POL'Y 247, 283 (2016) (analyzing text messages and direct social media messages under the Fourth Amendment and applying a modern-day-equivalent analysis), with Marc McAllister, *The Fourth Amendment and New Technologies: The Misapplication of Analogical Reasoning*, 36 S. ILL. U. L.J. 475, 504–05 (2012) (analyzing text messages under the Fourth Amendment and rejecting a modern-day-equivalent analysis). See Robin Miller, Annotation, *Expectation of Privacy in Text Transmissions to or from Pager, Cellular Telephone, or Other Wireless Personal Communications Device*, 25 A.L.R. 6th 201 (2007) (aggregating pre-*Carpenter* Fourth Amendment cases about text messages).

257. *Riley v. California*, 134 S. Ct. 2473 (2014).

258. *Id.* at 2488; *Carpenter v. United States*, 138 S. Ct. 2206, 2219 (2018).

A. Rejecting Conventional Analogies

In *Riley*, the Chief Justice famously and dismissively said:

The United States asserts that a search of all data stored on a cell phone is “materially indistinguishable” from searches of these sorts of physical items [such as billfolds, address books, purses, and wallets]. That is like saying a ride on horseback is materially indistinguishable from a flight to the moon. Both are ways of getting from point A to point B, but little else justifies lumping them together.²⁵⁹

This is a surprising, wholesale rejection of a conventional analogy: the government urged the Court to compare a digital technology to a physical world precursor, and the Court not only refused to do so but responded with sarcastic exaggeration. Understanding this quote is the key to understanding both *Riley* and *Carpenter* and, more broadly, the key to understanding how profoundly these cases have transformed the way the Court will reason through Fourth Amendment cases.

The horseback quote is only the most extreme example of the Court refusing to draw an analogy to an ordinary, physical world item or activity. The Court similarly dispenses with many other traditional analogies: a search through a cell phone is not like rifling through pockets;²⁶⁰ the term “cell phone” itself is misleading, because these are “minicomputers that also happen to have the capacity to be used as a telephone”;²⁶¹ and accessing CSLI is nothing like tailing a car.²⁶²

The Court did embrace some analogies in these opinions, but these tended to feel far more fanciful than the ones it rejected, drawn essentially from science fiction rather than conventional reality. Cell phones might be mistaken by aliens to be “features of human anatomy”;²⁶³ tracking CSLI is akin to “attaching an ankle monitor to the phone’s user”;²⁶⁴ searching through a cell phone is more invasive than searching through a house.²⁶⁵

Legal scholars have long analyzed the critical role of reasoning by analogy to legal reasoning.²⁶⁶ Judges decide cases by determining

259. *Riley*, 134 S. Ct. at 2488 (citations omitted).

260. *Id.* at 2484, 2489.

261. *Id.* at 2489.

262. *Carpenter*, 138 S. Ct. at 2218.

263. *Riley*, 134 S. Ct. at 2484.

264. *Carpenter*, 138 S. Ct. at 2218.

265. *Riley*, 134 S. Ct. at 2490–91.

266. See, e.g., EDWARD H. LEVI, AN INTRODUCTION TO LEGAL REASONING (2d ed. 2013); LLOYD L. WEINREB, LEGAL REASON: THE USE OF ANALOGY IN LEGAL ARGUMENT (2005); Cass R. Sunstein, *On Analogical Reasoning*, 106 HARV. L. REV. 741 (1993); Frederick

whether new fact pattern X is similar to previously analyzed fact pattern Y in relevant respects.²⁶⁷ Analogical reasoning gains force in legal reasoning because it is the “usual form of reasoning in daily life.”²⁶⁸

In Fourth Amendment jurisprudence, analogies play a dominant role. Tracking beepers are like following a car on city streets;²⁶⁹ hidden microphones are like human memory;²⁷⁰ and pen registers are like human telephone operators.²⁷¹ The *Carpenter* Court’s rejection of conventional analogies is thus a significant development. By refusing to credit the government’s preferred analogies, the Court could distinguish *Smith* and *Miller* without needing to overturn the forty-year-old precedents.

How *Carpenter* and *Riley* have treated analogy and precedent might be their most important and lasting revolution. The Court seems to be signaling that a foundation stone of legal reasoning — drawing comparisons to the ordinary, physical stuff of life — can be called into question. We are all now living in a science fictional universe, at least when making arguments to the Court. Why has the Court made this move, is it justified, and what does it mean for Fourth Amendment law going forward?

B. The Chief Justice’s Tech Exceptionalism

What causes these analogies to fail, in the eyes of the Court, is the nature of the technological era in which we are living. The Chief Justice has declared in successive landmark decisions that the information age has produced technological changes that are different in kind not merely in degree from the technology of the past.²⁷² He first announced this worldview, writing for eight justices, in *Riley v. California*, which held that the police need a warrant to search the contents of a cell phone incident to a valid arrest.²⁷³ In *Carpenter*, he exhibits the same beliefs, this time to even more consequential doctrinal import.

Schauer, *Analogy in the Supreme Court: Lozman v. City of Riviera Beach, Florida*, 2013 SUP. CT. REV. 405, 407 (2014).

267. Sunstein, *supra* note 266, at 745.

268. *Id.* at 743.

269. *United States v. Knotts*, 460 U.S. 276, 285 (1983) (comparing the use of a tracking beeper to following a suspect in a police car).

270. *United States v. White*, 401 U.S. 745, 751 (1971) (comparing a hidden microphone to an informant who writes down what he has heard).

271. *Smith v. Maryland*, 442 U.S. 735, 744 (1979) (comparing automatic telephone switching information to a human operator).

272. *See, e.g., Riley v. California*, 134 S. Ct. 2473, 2488 (2014) (“The United States asserts that a search of all data stored on a cell phone is ‘materially indistinguishable’ from searches of these sorts of physical items. That is like saying a ride on horseback is materially indistinguishable from a flight to the moon.”).

273. *Id.* at 2485.

The Chief Justice writes these opinions with what feels to me like a palpable, wide-eyed amazement at the speed with which the power and scale of technology has changed. In *Riley*, he marvels that in the five short years from arrest to Supreme Court ruling, the world had rendered obsolete the flip phone used by one of the defendants in the cases being reviewed.²⁷⁴ Similarly, in *Carpenter* he compares with astonishment the costly task of tracking a person's location on foot to the efficiency of doing so by downloading their CSLI.²⁷⁵

He emphasizes the sheer scale of modern technology. These opinions are replete with mentions of the word “millions” — “millions of pages of text;”²⁷⁶ “over a million apps available;”²⁷⁷ “396 million cell phone service accounts in the United States — for a nation of 326 million people”;²⁷⁸ and a database automatically tracking the location of “400 million devices.”²⁷⁹

Some of the words and phrases used in these opinions would seem more at home in science fiction than the U.S. Reports. These opinions invoke time travel,²⁸⁰ space travel,²⁸¹ and visits from Martians.²⁸²

The Chief Justice is equally impressed with the social dynamics of technological change — the rate with which technology like the smartphone has been adopted by Americans and has shaped our social interactions. In both opinions, he cites statistics and surveys demonstrating the large percentage of Americans who use these devices.²⁸³ He punctuates both with a statistic that has clearly left a lasting impression: “12% [of smartphone owners] admit[] that they even use their phones in the shower.”²⁸⁴

The Chief Justice connects this tech exceptionalism into Fourth Amendment doctrine with this key move: the “[m]odern cell phones are not just another technological convenience. With all they contain and all they may reveal, they hold for many Americans, the privacies of

274. *Id.* at 2484.

275. *Carpenter v. United States*, 138 S. Ct. 2206, 2217–18 (2018).

276. *Riley*, 134 S. Ct. at 2489.

277. *Id.* at 2490.

278. *Carpenter*, 138 S. Ct. at 2211.

279. *Id.* at 2218.

280. *Id.*

281. *Riley*, 134 S. Ct. at 2488.

282. *Id.* at 2484.

283. *Id.* at 2490 (citing statistic that 90% of American adults who own a cell phone use it to store private documents); *Carpenter*, 138 S. Ct. at 2211 (noting that Americans own 396 million cell phones, meaning more devices than people).

284. *Riley*, 134 S. Ct. at 2490 (citing HARRIS INTERACTIVE, 2013 MOBILE CONSUMER HABITS STUDY (2013), <https://web.archive.org/web/20130715020841/http://www.jumio.com/2013/07/where-do-you-take-your-phone/>); *Carpenter*, 138 S. Ct. at 2218. Do these people simply use their phone next to their shower to listen to audio inside the shower, or are they wrapping their device in a waterproof pouch and bringing it in with them? The Chief Justice does not say.

life.”²⁸⁵ Nothing that has come before can compare to these devices for the amount and variety of sensitive and intimate information about individuals.²⁸⁶ In the passage perhaps most bristling with constitutional import in these opinions, the Chief Justice declares that a person’s privacy interest in the contents of a smartphone is more significant than the privacy interest in a home, the ancient, paradigmatic high-water mark for privacy.²⁸⁷

What flows directly from the conclusion that these devices are unprecedented vessels for sensitive information is the recognition that technology has significantly increased the power of the police.²⁸⁸ Keeping with the science fiction theme, these devices and the records they produce essentially transform the police into crime-fighting robots outfitted with superhuman powers. They can peer into the past, avoiding the “frailties of recollection.”²⁸⁹ They can tail every suspect “every moment of every day for five years.”²⁹⁰ They are “tireless,”²⁹¹ “ever alert, and their memory is nearly infallible.”²⁹²

All of this powerful rhetoric about the power of technology has a profound impact on the reasoning of the Court by allowing it to discard analogies to what have come before. For an institution that places historical continuity, *stare decisis*, and analogical reasoning at its core, the Court’s recent refusals to accept straightforward analogies is jarring.

C. The Argument for Tech Exceptionalism

The Court’s adoption of tech exceptionalism is not science fiction; it is well justified. Changes in technology in recent years have posed challenges to privacy that are different in kind not merely in degree than what has come before. Advances in the past two decades, in particular, have dramatically decreased the ability with which individuals can understand, much less control, the ways they are observed and even controlled.

Ryan Calo has written about the tech exceptionalism of our time.²⁹³ He argues that the field of cyberlaw is premised on the idea that fundamental advances in technology such as the Internet or robotics are so qualitatively and quantitatively different from what has come before

285. *Riley*, 134 S. Ct. at 2494–95.

286. *Id.* at 2489–90.

287. *Id.* at 2491 (“[I]t also contains a broad array of private information never found in a home in any form — unless the phone is.”).

288. Kerr, *Equilibrium*, *supra* note 73, at 480.

289. *Carpenter v. United States*, 138 S. Ct. 2206, 2218 (2018).

290. *Id.*

291. *Id.*

292. *Id.* at 2219.

293. Ryan Calo, *Robotics and the Lessons of Cyberlaw*, 103 CALIF. L. REV. 513, 550–51 (2015).

that they force changes in the law.²⁹⁴ Specifically, “a technology is exceptional when its introduction into the mainstream requires a systematic change to the law or legal institutions in order to reproduce, or if necessary displace, an existing balance of values.”²⁹⁵ This is precisely what the Chief Justice argued that the smartphone and CSLI have wrought.

The Chief Justice’s arguments are backed by two decades of scholarly writing. This is perhaps best seen in the output of the annual Privacy Law Scholars Conference (“PLSC”), now in its twelfth year.²⁹⁶ The authors attending this conference have presented almost six hundred articles, the vast majority of which have argued that specific changes in technology have threatened information privacy.²⁹⁷

Articles presented at PLSC establish that technological advances increase the quantity and quality of information available to third parties.²⁹⁸ They highlight the role inference plays in disrupting settled expectations of privacy, because it is no longer enough to look at what is literally in the data;²⁹⁹ advances in technology such as machine learning give individuals the power to learn more than what is on the surface.³⁰⁰

PLSC articles have documented how these advances consistently thwart expectations and put pressure on social norms.³⁰¹ A massive literature chronicles the harms that these incursions into privacy have wrought, either on individuals, groups, or institutions.³⁰² Many articles have identified harms that go beyond traditional injury to harms that interfere with autonomy and personal development.³⁰³ Other articles discuss the futility of self-help techniques for addressing these risks.³⁰⁴

294. *Id.* at 553–58.

295. *Id.* at 552.

296. 2018 Privacy Law Scholars Conference (PLSC2018), BERKELEY LAW, <https://www.law.berkeley.edu/research/bclt/bcltevents/2018annual-privacy-law-scholars-conference> [<https://perma.cc/DXK8-BFAE>].

297. Data on file with author.

298. See, e.g., DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE 213 (2006).

299. Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701, 1703–04 (2010).

300. Steven M. Bellovin et. al., *When Enough Is Enough: Location Tracking, Mosaic Theory, and Machine Learning*, 8 NYU J.L. & LIBERTY 556, 560 (2014).

301. See, e.g., HELEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE (2009).

302. Daniel J. Solove & Danielle Keats Citron, *Risk and Anxiety: A Theory of Data-Breach Harms*, 96 TEX. L. REV. 737, 739 (2018); M. Ryan Calo, *The Boundaries of Privacy Harm*, 86 IND. L.J. 1131, 1133 (2011); Ohm, *Sensitive Information*, *supra* note 87, at 1196.

303. JULIE E. COHEN, CONFIGURING THE NETWORKED SELF: LAW, CODE, AND THE PLAY OF EVERYDAY PRACTICE 223–25 (2012); Neil M. Richards, *Intellectual Privacy*, 87 TEX. L. REV. 387, 389 (2008); Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609, 1613 (1999).

304. Daniel J. Solove, *Introduction: Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1879, 1880–81 (2013); see Aleecia M. McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, 4 I/S: J. L. & POL’Y FOR INFO. SOC’Y 543, 564 (2008).

It is fair to say that almost no scholarly writing refutes the argument that recent changes in technology have put significant pressure on privacy and privacy law. The very small number of detractors or skeptics who write in the field tend to argue instead that the harms are either poorly supported by empirics or outweighed by the harm that would be caused by changes to the law.³⁰⁵

Thus, Chief Justice Roberts's adoption of tech exceptionalism finds support from a significant body of scholarly argument. Far from being just the unfounded opinion of a sixty-something jurist,³⁰⁶ tech exceptionalism is an argument well within the mainstream of contemporary academic writing in privacy law.

D. Expertise and Analogy

Having established that Chief Justice Roberts views modern technology as exceptional, and having defended this view, I ask, how does this view lead him to disregard analogy and break with the Court's precedents? How does tech exceptionalism change Fourth Amendment jurisprudence? When tech exceptionalism collides with the legal system, it creates a fundamental problem of expertise. Non-technical lawyers are simply not trained to explicate the ways in which fundamental changes in complex technology put pressure on privacy and increase government power.³⁰⁷ They need to seek help from outside experts. This is especially necessary when the complex technology continues to change, presenting not only a complex target of analysis, but a moving one.

This leaves the Court needing to turn to unusual sources of technological explication.³⁰⁸ *Riley* cites multiple amici briefs for complex details about technology that were never entered into the lower court

305. Lior Jacob Strahilevitz, *Privacy Versus Antidiscrimination*, 75 U. CHI. L. REV. 363, 364 (2008); Adam Thierer, *Privacy Law's Precautionary Principle Problem*, 66 ME. L. REV. 467, 468 (2014); Eugene Volokh, *Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People from Speaking About You*, 52 STAN. L. REV. 1049, 1049 (2000); Jane Yakowitz, *Tragedy of the Data Commons*, 25 HARV. J.L. & TECH. 1, 3–4 (2011).

306. Strahilevitz, *Ten Thoughts*, *supra* note 2 (“The majority text and approach are consistent with the Chief’s dim views about legal scholarship generally and with his stated preference for minimalist decisions.”).

307. See Calo, *supra* note 293, at 560 (describing the “tradition of melding legal and technical expertise” in Cyberlaw).

308. Milligan, *supra* note 69, at 1336–37 (arguing that public interest groups and litigants should educate courts when simple analogies fail).

record.³⁰⁹ It cites to reports by government agencies known for objective scientific expertise.³¹⁰ It also contains what is probably the first Supreme Court citation ever to a smartphone operating system manual.³¹¹

Carpenter cites fewer external sources for technological facts than *Riley*, in part because it can cite *Riley* for some of its facts.³¹² Still, the majority opinion's only citation to an amicus brief is to one authored by digital civil rights groups, including the Electronic Frontier Foundation, which provides critical information about the improved precision of cell tower tracking techniques since the facts of the case were first established.³¹³

Tech exceptionalism's expertise problem explains and justifies the Court's rejection of the simplistic, conventional analogies offered by the government in *Riley* and *Carpenter*, such as the refusal to compare a smartphone to an address book.³¹⁴ In order to make proper sense of an analogy comparing an old X to a new Y, one must be expert enough to understand the relevant similarities and differences between X and Y.

This connection between analogy and expertise has been explored by legal scholars to support the argument that lawyers can sometimes see analogies that non-lawyers cannot. Frederick Schauer and Barbara Spellman offer one account.³¹⁵ A lawyer who specializes in First Amendment doctrine can see instantly the relevant similarities between self-described "Nazis" in the National Socialist Party of America and "civil rights demonstrators of the 1960s," a comparison the non-lawyer might see as "bizarre, even offensive."³¹⁶ The domain-specific expertise of First Amendment law makes apparent the similarities of these

309. *Riley v. California*, 134 S. Ct. 2473, 2486 (2014) (citing Brief of United States as amicus curiae about unbreakability of iPhone encryption); *id.* at 2487 (citing Brief for Criminal Law Professors about law enforcement use of "Faraday bags"); *id.* at 2489 (citing Brief for Center for Democracy & Technology about amount of physical world document equivalent to 16 gigabytes of digital storage); *id.* at 2490 (citing Brief for Electronic Privacy Information Center about number of smartphone apps installed by the average user).

310. *Id.* at 2486 (citing report by National Institute for Standards and Technology); *id.* at 2487 (citing report by National Institute of Justice).

311. *Id.* at 2487 (citing iPhone User Guide for iOS 7.1 Software 10 (2014)).

312. See *Carpenter v. United States*, 138 S. Ct. 2206, 2214 (2018) (citing *Riley*, 134 S. Ct. 2473, about "'immense storage capacity' of modern cell phones"); *id.* at 2218 (citing *Riley*, 134 S. Ct. 2473, for cell phone ownership and use statistics).

313. See *id.* at 2219 ("[W]ith new technology measuring the time and angle of signals hitting their towers, wireless carriers already have the capability to pinpoint a phone's location within 50 meters.") (citing Brief for Electronic Frontier Foundation et al.).

314. McAllister, *supra* note 256, at 475, 477 ("In rejecting Fourth Amendment claims involving warrantless use of sophisticated technologies, courts often rely upon analogies to prior 'search' cases, but these supposed analogies are so far removed from the new forms of surveillance that analogies to them only confuse, rather than clarify, the actual analysis required by Katz." (sic)).

315. Frederick Schauer & Barbara A. Spellman, *Analogy, Expertise, and Experience*, 84 U. CHI. L. REV. 249, 264–65 (2017).

316. *Id.* at 264–65.

groups whose wish to march in public places was opposed by viewpoint-based laws.³¹⁷

Tech exceptionalism turns the tables on lawyers, relegating them to the role of non-experts who cannot understand the failure of a given analogy because they cannot accurately characterize Y or compare it to X when complicated technology is involved.³¹⁸ Luke Milligan argues that when faced with complex technology in surveillance cases, courts should deploy an “analogy breaker” rejecting misleading analogies in favor of a “fresh ‘default’ analysis.”³¹⁹

The challenge for criminal lawyers and scholars going forward is to grapple with the nuances of technology. The Court now places great emphasis on the subtle intricacies of how technology operates, and how it differs in important ways from what has come before. We need to look to computer scientists and engineers to serve as experts and to write legal scholarship to help guide the way.³²⁰ But this is not simply a scientific or engineering exercise; the Court cares also about how humans and groups use technology. This gives impetus on new interdisciplinary bridges between law and fields such as Science and Technology Studies and Human-Computer Interaction.³²¹

The Court’s new focus on the legitimate and appropriate sources of facts should spur some modest institutional changes. Both prosecutors and defense lawyers now need sophisticated technological support, either in the form of dedicated technologists or, at the very least, hybrid-trained lawyers with some experience in technology. Civil liberties groups will need to continue their trend of hiring in-house technologists. It is not a coincidence that many of the amici briefs cited by the Court were authored by groups focused on digital civil rights and well known for hiring and associating with trained technologists.³²²

Finally, this shift should encourage legal scholars who write about the Fourth Amendment and technology to place a premium on getting

317. *Id.*

318. *See id.* at 266–67 (arguing that the domain-specific knowledge of experts allows them to see analogies that non-experts do not).

319. Milligan, *supra* note 69, at 1334–35. Milligan weighs this proposal down with concepts of “mono-analogical” and “poly-analogical” features of comparisons. *Id.* at 1324–35. Although I do not find these to be useful additions to the theory, Milligan’s bottom line is that courts should not rely too heavily on simplistic analogies when dealing with emerging technologies.

320. *See* Calo, *supra* note 293, at 561 (“Whether at conferences or hearings, in papers or in draft legislation, the legally and technically savvy will need to be in constant conversation.”).

321. *See generally* SERGIO SISMONDO, AN INTRODUCTION TO SCIENCE AND TECHNOLOGY STUDIES (2d ed. 2010); JEFF JOHNSON, DESIGNING WITH THE MIND IN MIND: SIMPLE GUIDE TO UNDERSTANDING USER INTERFACE DESIGN RULES (1st ed. 2010).

322. *See* *Riley v. California*, 134 S. Ct. 2473, 2489 (2014) (citing Brief for Center for Democracy & Technology et al.); *id.* at 2490 (citing Brief for Electronic Privacy Information Center et al.); *Carpenter v. United States*, 138 S. Ct. 2206, 2219 (2018) (citing Brief for Electronic Frontier Foundation et al.).

the technological details right. The only law review article cited in either majority opinion was authored by Orin Kerr, who is not only a preeminent scholar but also one with formal technological training and experience;³²³ and many of the majority's arguments echo themes found in uncited articles, also written by trained or technologically sophisticated legal scholars.³²⁴

E. Time and Technological Change

The unprecedented, rapidly changing nature of technology also causes the Court to relax its rules about restricting its attention to the record evidence before it. Traditionally, appellate courts, including the Supreme Court, refuse to peek outside the record developed in the trial court. Some of this reticence comes from Article III of the Constitution, which limits federal courts to consider only "cases" or "controversies."³²⁵ But it also reflects an institutional modesty that recognizes that appellate courts are distant from the facts.

Tech exceptionalism puts pressure on this understanding. The premise of tech exceptionalism is that technology changes today at unprecedented rates. An appellate court that looks only to the past is using the outdated examples in the record to set rules for the present and future, which might already differ in important ways. In *Carpenter* and *Riley*, the Court refused to resign itself to this fate. Instead, it relaxed, just slightly, its practices by peeking a little at the present and the future.

This leads to three new principles of judicial fact-finding: refresh what has changed during the pendency of litigation and appeal; relax the rules of judicial notice; and understand that the future is ascertainable.

First, the Court in these opinions shows a willingness to refresh the record, a little, at each stage of appeal. It takes several years to proceed from an arrest, through appeals, to review by the Supreme Court.³²⁶ Given the rate of change of technology, the passage of time means the Court will often be reviewing historical relics in cases like these. The

323. See *Riley*, 134 S. Ct. at 2489 (citing Orin Kerr, *Foreword: Account for Technological Change*, 36 HARV. J.L. & PUB. POL'Y 403, 404–05 (2013)). Professor Kerr has undergraduate and graduate degrees in engineering. Curriculum Vitae of Orin S. Kerr, USC GOULD, https://gould.usc.edu/portal/directory/photos/Kerr_Orin_CV.pdf [<https://perma.cc/JZJ7-JYRT>].

324. See, e.g., Kevin S. Bankston & Ashkan Soltani, *supra* note 70, at 335; Freiwald, *First Principles*, *supra* note 33; Henderson, *supra* note 63.

325. U.S. CONST. art. III, § 2.

326. In *Riley*, the defendants in the two cases reviewed were arrested in August 2009 and September 2007, respectively. Petition for Writ of Certiorari at 1–2, *Riley*, 134 S. Ct. 2473 (No. 13-132); *United States v. Wurie*, 728 F.3d 1, 1–2 (1st Cir. 2013). The Supreme Court decided the cases on June 25, 2014, almost five and seven years after the arrests, respectively. *Riley*, 134 S. Ct. at 2473. In *Carpenter*, the first co-conspirators were arrested in April 2011, *United States v. Carpenter*, 819 F.3d 880, 884 (6th Cir. 2016), seven years before the Supreme Court's decision. *Carpenter*, 138 S. Ct. at 2206.

Court has responded by seeing fit to peek at the present, availing itself of the kind of unusual sources of information listed above, including amici.

Second, the Court also seems willing to relax its ordinary attitudes about taking judicial notice. In *Riley*, the Court cited the iPhone User Guide for the proposition that “most phones lock at the touch of a button or, as a default, after some very short period of inactivity,”³²⁷ a citation criticized by observers.³²⁸ This extra-record “fact” was introduced to the Court through an amici brief filed by the United States in support of the State of California.³²⁹ Although the Court does not explicitly acknowledge that it is taking judicial notice³³⁰ of this technological fact, this seems to be what it has done.

Finally, the Court is not afraid to look past the facts of the technology at issue before it to the present and likely near-future technology that we will soon encounter. The Court implies that the future is ascertainable; it is something we can talk about and predict with some certainty. In *Carpenter*, the Court assessed how cell-site technology had changed in the intervening seven years.³³¹ In *Riley*, the Court noted how the flip phone at issue had already “faded in popularity.”³³²

This sets up a rather stark departure from Justice Kennedy’s approach in *City of Ontario v. Quon*,³³³ a 2010 opinion that held that a government employer’s review of an employee’s text messages on a work pager was reasonable.³³⁴ Justice Kennedy cautioned that the Court “risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear.”³³⁵ In *Carpenter*, Chief Justice Roberts prefers the *Kyllo* attitude toward predicting the future: we “must take account of more sophisticated systems that are already in use or in development.”³³⁶

327. *Riley*, 134 S. Ct. at 2487.

328. See, e.g., H. Adam Shapiro, *Court Continues to Misunderstand How We Use Technology*, DANZINGER, SHAPIRO & LEAVITT BLOG (June 25, 2014), <https://www.ds-l.com/blog/2014/06/the-supreme-court-continued-it.html> [<https://perma.cc/4G3L-Y3GK>].

329. See Brief for the United States as Amici Curiae Supporting Respondent at 11, *Riley*, 134 S. Ct. 2473 (No. 13-132), 2014 WL 1389032.

330. See FED. R. EVID. 201 (allowing federal courts to take judicial notice of facts that “can be accurately and readily determined from sources whose accuracy cannot reasonably be questioned”).

331. *Carpenter*, 138 S. Ct. at 2219 (noting how more cell towers and better technology had brought the accuracy of CSLI closer to that of GPS).

332. *Riley*, 134 S. Ct. at 2484.

333. 560 U.S. 746 (2010).

334. *Id.* at 761.

335. *Id.* at 759.

336. *Carpenter*, 138 S. Ct. at 2218–19 (quoting *Kyllo v. United States*, 533 U.S. 27, 36 (2001)).

F. Refusing to Look Backwards

The Court decided to look to the future in the face of many urging it to look to the past. Scholars urged the Court to base its Fourth Amendment decisions on a close examination of, in turn, survey evidence, history, or sources of positive law. The Court ignored all of this advice, much to the consternation of the scholars involved.

1. The Surveyors

The objective prong of the REP test asks whether an expectation of privacy is “one that society is prepared to recognize as ‘reasonable.’”³³⁷ Some have read the prong to hitch the Fourth Amendment’s protections to public sentiment.³³⁸ Police power respected the bounds of constitutional privacy so long as it did not stray too far from what ordinary people or average people expect.³³⁹ The REP test should produce results that follow, at least to some extent, what people actually expect, or so these observers have argued.³⁴⁰

For those who would connect REP to the attitudes of ordinary people, the next step was to survey Americans, gathering opinions about various police practices, including many fact patterns that have already been the subject of Supreme Court case law. This originated with landmark work in the late 1990’s by Christopher Slobogin and Joseph Schumacher.³⁴¹ Through their surveys, the pair concluded that public sentiment about the invasiveness of police practice disagreed in many instances with the Court’s Fourth Amendment doctrine.³⁴² For example, the survey respondents judged “perus[ing] bank records” to be the thirty-eighth most invasive activity out of fifty surveyed, roughly the same as “hospital surgery on shoulder,”³⁴³ contradicting the relative holdings of *Miller* and *Winston v. Lee*.³⁴⁴

The turn to survey work has been revived and invigorated in recent years.³⁴⁵ A chief advocate is Lior Strahilevitz, working with Matthew

337. *Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

338. Kugler & Strahilevitz, *Actual Expectations*, *supra* note 184, at 243.

339. *See Smith v. Maryland*, 442 U.S. 735, 740, 742 (1979).

340. *See Kugler & Strahilevitz, Actual Expectations*, *supra* note 184, at 224–25.

341. Christopher Slobogin & Joseph E. Schumacher, *Reasonable Expectations of Privacy and Autonomy in Fourth Amendment Cases: An Empirical Look at Understandings Recognized and Permitted by Society*, 42 DUKE L.J. 727, 728 (1993).

342. *Id.* at 740.

343. *Id.* at 738–40.

344. *Compare United States v. Miller*, 425 U.S. 435, 444 (1976) (holding that obtaining bank records was not a search), with *Winston v. Lee*, 470 U.S. 753, 759–63 (1985) (requiring probable cause plus additional factors for surgery in shoulder).

345. *See Bernard Chao et al., Why Courts Fail to Protect Privacy: Race, Age, Bias, and Technology*, 106 CALIF. L. REV. 263, 266 (2018); Chris Jay Hoofnagle & Jennifer M. Urban, *Alan Westin’s Privacy Homo Economicus*, 49 WAKE FOREST L. REV. 261, 262 (2014); Matthew B. Kugler & Lior Jacob Strahilevitz, *The Myth of Fourth Amendment Circularity*, 84 U.

Kugler.³⁴⁶ Strahilevitz and Kugler have written two articles reporting the results of two surveys they have conducted.³⁴⁷ The authors spend much more time than Slobogin and Schumacher trying to lay out a doctrinal and normative case for why judges ought to look to surveys when assessing police practices.³⁴⁸ They cite democratic legitimacy, doctrinal coherence and predictability, and the costs of creating legal rules that ordinary citizens don't understand or expect as the primary justifications.³⁴⁹ This work follows the broader trend in legal scholarship of finding new roles and contexts for quantitative social science.³⁵⁰

These scholars, joined by others who have published surveys about privacy attitudes, wrote an amicus brief urging the *Carpenter* Court to look to the evidence they had gathered.³⁵¹ The brief summarizes results showing that very few Americans are aware of the ability of cell phone companies to track the location of phones using CSLI, supporting an argument for requiring a warrant in the case.³⁵²

The majority opinion failed to cite any of the survey evidence in its opinion. The survey work did appear in some of the dissents, albeit in support of only minor arguments.³⁵³

Strahilevitz has been among the sharpest critics of the majority opinion's reasoning, if not its result.³⁵⁴ He faults the opinion not just

CHI. L. REV. 1747, 1751 (2017) [hereinafter Kugler & Strahilevitz, *The Myth*]; Christine S. Scott-Hayward et al., *Does Privacy Require Secrecy? Societal Expectations of Privacy in the Digital Age*, 43 AM. J. CRIM. L. 19, 22 (2015); Kugler & Strahilevitz, *Actual Expectations*, *supra* note 184, at 245; Matthew Tokson, *Knowledge and Fourth Amendment Privacy*, 111 NW. U. L. REV. 139, 144 (2016).

346. See Kugler & Strahilevitz, *The Myth*, *supra* note 345; Kugler & Strahilevitz, *Actual Expectations*, *supra* note 184.

347. Kugler & Strahilevitz, *The Myth*, *supra* note 345; Kugler & Strahilevitz, *Actual Expectations*, *supra* note 184.

348. See Kugler & Strahilevitz, *Actual Expectations*, *supra* note 184, at 224–27.

349. *Id.*

350. See Lee Epstein & Gary King, *The Rules of Inference*, 69 U. CHI. L. REV. 1, 3 (2002). Strahilevitz teaches at the University of Chicago, the cradle of law and economics. His arguments for incorporating surveys into the Fourth Amendment expressly rely on principles from law and economics. See Kugler & Strahilevitz, *Actual Expectations*, *supra* note 184, at 227 (advocating a normative framework for the Fourth Amendment that “enhance[s] social welfare” and does not spur people to “take excessive precautions to protect their information”); *id.* (“[W]e think there is a strong case to be made that misalignment between the law and societal expectations is detrimental for both efficiency and fairness-related reasons.”).

351. Brief for Empirical Fourth Amendment Scholars as Amici Curiae Supporting Petitioner, *Carpenter v. United States*, 138 S. Ct. 2206 (2018) (No. 16-402), 2017 WL 3530963.

352. *Id.* at *3 (citing study showing that only 26.5% of American cell phone users expressed even a general awareness about location tracking by cell phone companies).

353. *Carpenter v. United States*, 138 S. Ct. 2206, 2244 n.10 (2018) (Thomas, J., dissenting) (citing Kugler & Strahilevitz, *Actual Expectations*, *supra* note 184, at 241, among others, to demonstrate scholarly disapproval of the *Katz* test); *id.* at 2265 (Gorsuch, J., dissenting) (citing Slobogin & Schumacher, *supra* note 341, at 732, 740–42 for proposition that “judicial judgments often fail to reflect public views”).

354. See Strahilevitz, *Ten Thoughts*, *supra* note 2.

for failing to cite survey work but for more broadly refusing to engage legal scholarship.³⁵⁵

2. The Legal Historians

One notable legal historian who has focused on the Fourth Amendment in recent years is Laura Donohue, who has advocated for what might be described as an expansive originalism for the Fourth Amendment.³⁵⁶ In her carefully researched, book-length article, Donohue excavates English and colonial law, as well as the story of the drafting of the Constitution and Bill of Rights, to take on misimpressions of Fourth Amendment history.³⁵⁷

Professor Donohue also joined an amicus brief in *Carpenter* that was filed by a group of “scholars of the history and original meaning of the Fourth Amendment.”³⁵⁸ The historians argued that rummaging through CSLI fits the meaning of the word “search” at the time of the founding and analogized the search of CSLI as akin to the use of general warrants that motivated the Revolution and the drafters of the Bill of Rights.³⁵⁹ They noted how the early, celebrated cases of *Wilkes v. Wood*³⁶⁰ and *Entick v. Carrington*³⁶¹ involved opinions that focused on how searches created invasions into privacy and personal affairs.³⁶²

The majority opinion engages in almost no historical analysis, beyond an obligatory acknowledgement of the role the opposition to general warrants and writs of assistance played in sparking the American Revolution.³⁶³ Justices Thomas and Gorsuch engaged the history much more deeply in their respective dissents. Only Justice Thomas cites the work of legal historians, including Donohue and Cuddihy, while using the history to conclude that no search had occurred in this case — the opposite conclusion the historians pressed in their brief.³⁶⁴

355. *Id.*

356. See Laura K. Donohue, *The Original Fourth Amendment*, 83 U. CHI. L. REV. 1181, 1193 (2016).

357. *Id.* at 1193–95.

358. Brief for Scholars of the History and Original Meaning of the Fourth Amendment as Amici Curiae Supporting Petitioner, *Carpenter v. United States*, 138 S. Ct. 2206 (2018) (No. 16-402), 2017 WL 3530961. Among the other signers of the historians’ brief was William Cuddihy, author of a well cited, exhaustive history of the Fourth Amendment. See WILLIAM J. CUDDIHY, *THE FOURTH AMENDMENT: ORIGINS AND ORIGINAL MEANING* (2009).

359. Brief for Scholars, *supra* note 358, at 3.

360. (1763) 98 Eng. Rep. 489 (PC).

361. (1765) 95 Eng. Rep. 807 (KB).

362. CUDDIHY, *supra* note 358, at 9–10.

363. *Carpenter v. United States*, 138 S. Ct. 2206, 2213 (2018).

364. *Id.* at 2243 (Thomas, J., dissenting) (citing Cuddihy and Donohue); *id.* at 2240 (citing Donohue); *id.* at 2241 (same).

3. The Positive Law Proponents

Finally, much attention has been paid to a recent law review article by William Baude and James Stern.³⁶⁵ The authors propose a dramatically simplified question to replace the REP: “have [officials] engaged in an investigative act that would be unlawful for a similarly situated private actor to perform”?³⁶⁶ If yes, a search has occurred; if not, no search has occurred.³⁶⁷ The sources of illegality would include property law — thus bearing some resemblance to Justice Scalia’s rule in *Jones* — but would go beyond to include “any prohibitory legal provisions, whether legislative, judicial, or administrative in origin, and whether classified as criminal or civil in nature.”³⁶⁸

The authors argue that confining the meaning of search to issues addressed in the positive law is better than the REP test because “[i]t is conceptually clear, theoretically sound, less subjective, more legal, and responsive both to social fact and technological change.”³⁶⁹ They connect the proposal to historical references to positive law in critiques of British search and seizure practice; the structural advantages of making Fourth Amendment law act similarly to Fifth Amendment takings jurisprudence; and the idea that judging the police by the same laws that govern us all contributes to the rule of law.³⁷⁰ Finally, they point to practical advantages, touting that it betters the REP test by being clearer, equally adaptable, and more respectful of the role of the legislature.³⁷¹

Neither Baude nor Stern signed an amicus brief, but their article was cited in the Petitioner’s opening brief.³⁷² Although the majority opinion failed to cite the article, it was cited in the dissents by both Justices Thomas and Gorsuch.³⁷³

4. Looking Forward Not Backward

The majority’s refusal to embrace surveys, legal history, or the positive law when applying the Fourth Amendment to new technology should be seen as an affirmative rejection of these proposals by five justices, rather than as indifference or an oversight. The reason, once

365. See William Baude & James Stern, *The Positive Law Model of the Fourth Amendment*, 129 HARV. L. REV. 1821 (2016).

366. *Id.* at 1825.

367. The rule would extend to seizures as well. *Id.* at 1830.

368. *Id.* at 1833.

369. *Id.* at 1888.

370. *Id.* at 1837–50.

371. *Id.* at 1850–55.

372. Brief for Petitioner at 22 n.10, 32, *Carpenter v. United States*, 138 S. Ct. 2206 (2018) (No. 16-402), 2017 WL 3575179.

373. *Carpenter v. United States*, 138 S. Ct. 2206, 2242 (2018) (Thomas, J., dissenting); *id.* at 2268 (Gorsuch, J., dissenting).

again, is tech exceptionalism. Seen through this lens, approaches that look backward in time, like these three, do not serve a useful purpose, for the focus should turn to the present and future. This is not to say that history, surveys, and positive law will never again figure into Fourth Amendment cases involving advances in information technology. But for now, the Court has turned its back on them.

Most directly, history seems the wrong tool for reasoning about these questions. Given the significant differences between CSLI tracking and the location tracking of a few decades ago, it seems especially unhelpful to wonder what the Framers would have thought about CSLI.

In *Riley* and *Carpenter*, history is invoked, but briefly and in passing. History seems useful to the modern Fourth Amendment only held at a distance and as a source of very general analogy. “The fact that technology now allows an individual to carry [a cell phone’s worth of] information in his hand does not make the information any less worthy of the protection for which the Founders fought.”³⁷⁴ The suggestion is that searching a cell phone is akin to “the reviled ‘general warrants’ and ‘writs of assistance’ of the colonial era.”³⁷⁵

The Fourth Amendment is “informed by historical understandings ‘of what was deemed an unreasonable search and seizure [when the Fourth Amendment] was adopted.’”³⁷⁶ It is meant to “secure ‘the privacies of life’ against ‘arbitrary power,’” and “a central aim of the Framers was ‘to place obstacles in the way of a too permeating police surveillance.’”³⁷⁷ These quoted passages are the sum total of the Court’s attention to history in these two landmark opinions, a far cry from what the historians had hoped to see.

The problem with survey results in an era of tech exceptionalism is that lay attitudes about rapidly changing technology are likely to be rapidly changing, unstable, and uninformed. It is one thing to look at survey results to ask whether Americans think the police ought to be able to hide a recording device on a confidential informant. Average Americans have had nearly a century to understand voice recording and millennia to have developed fixed opinions about misplaced confidences.³⁷⁸ This seems like the kind of technology-aided surveillance that a court might rely on a survey to assess. But asking average Americans to opine about cell-site location information or facial recognition or smart meters is simply not likely to produce informed opinions.³⁷⁹ At best, it will reflect still developing attitudes about misunderstood

374. *Riley v. California*, 134 S. Ct. 2473, 2495 (2014).

375. *Id.* at 2494.

376. *Carpenter*, 138 S. Ct. at 2214.

377. *Id.*

378. See, e.g., CUDDIHY, *supra* note 355, at 333 (discussing use of informants for securing warrants in the colonies).

379. See Freiwald, *First Principles*, *supra* note 33, at *25.

and changing technologies. To be fair, Strahilevitz suggests something similar in his work.³⁸⁰ Why we would hitch our constitutionally bestowed civil liberties to the quicksand of the median American's technology literacy defies common sense.

The situation for the positive law is even worse. It compounds the confusion the general public has about the social meaning of rapidly changing technology with the vagaries of the sclerotic legislative and judicial processes.³⁸¹ This is especially true when considering statutory privacy law. Many have decried the state of privacy legislation at the national and state levels today as failing properly to account for the harms that can be wrought by new technology.³⁸² The situation has become much worse in recent years, as technology companies have discovered Washington and today spend more than almost any industry lobbying Congress.³⁸³

To put it succinctly, applying the Fourth Amendment to information technology requires the Court to look forward; all three of the proposed approaches look backward instead.

V. CONCLUSION

Based on the new rule it announces, *Carpenter* is already on par with some of the most consequential Fourth Amendment cases of all time. But when one looks beyond the core rule to some of the other revolutions wrought in the opinion, one is left to conclude that *Carpenter* represents a fundamental shift, not merely an incremental adaptation. *Carpenter* turns the third-party doctrine inside out, eroding the requirement of government action as a core underpinning of the Fourth Amendment; it applies even when the government acts directly to collect information about many individuals in massive databases; it implicitly suggests three new rules of technological equivalence; it embraces a tech exceptionalism that permits a break from judicial precedent; and it begins the overdue project of replacing the *Katz* REP test.

380. Kugler & Strahilevitz, *Actual Expectations*, *supra* note 184, at 234–35 (“We do think that the case for placing real weight on survey responses is strongest when laypeople are being surveyed on issues that are familiar to them. For that reason, our surveys ask people about the sorts of technologies that they are likely to have encountered in the world . . .”).

381. See Richard M. Re, *The Positive Law Floor*, 129 HARV. L. REV. F. 313, 326–27 (2016) (critiquing the positive law model by pointing to many reasons legislatures might not have yet regulated a new technology, including “regulatory lag”).

382. See, e.g., Ohm, *Sensitive Information*, *supra* note 87, at 1127.

383. See Re, *supra* note 381, at 329 (discussing role of private interest groups in debates surrounding legislation regulating privacy in data); see also OPENSECRETS.ORG, 2017 TOP INDUSTRIES, <https://www.opensecrets.org/lobby/top.php?indexType=i&showYear=2017> [<https://perma.cc/QCF2-FSS8>].

On December 19, 1967, the day after the Court decided *Katz*, it probably was not yet clear what the Court had done.³⁸⁴ The decision was rightly seen as important, the culmination of almost forty years of scholarly commentary against the narrow trespass theory reasoning of *Olmstead v. United States*.³⁸⁵ What might have been seen at first as merely an important decision only later was rightfully recognized for the many revolutions it created.

What *Katz* did to *Olmstead*, *Carpenter* will do to *Katz*, transforming the Fourth Amendment into something fundamentally new. The Fourth Amendment has become the vessel for a civil right that, for the first time, responds flexibly and rapidly to the insistent challenges of new technology on privacy.

384. *Katz v. United States*, 389 U.S. 347, 347 (1967). See Anthony G. Amsterdam, *Perspectives on the Fourth Amendment*, 58 MINN. L. REV. 349, 383–85 (1974) (writing seven years after *Katz*, describing the evolution in how the case had by then been interpreted).

385. *Olmstead v. United States*, 277 U.S. 438, 568 (1928); see Winn, *supra* note 377, at 2 (“The *Olmstead* decision was very divisive, and the government’s use of wiretaps continued to be controversial.”).

From: LaCicero, Nicole
Sent: 13 Nov 2019 23:53:12 +0000
To: Giles, Margaret M
Subject: RE: Venntel - Geolocation Data Services Legal Review Process

I have a silly question regarding next steps. If DHS decides not to use geolocation, does ICE have to comply? Technically, there negative finding would be based on an assumption of risk and not prohibited by a legal or regulatory requirement.

Thanks, Nicole

Nicole LaCicero, J.D./Joint M.S. Cybersecurity
Management and Program Analyst
Office of Information Governance and Privacy, Privacy Division
U.S. Immigration and Customs Enforcement
Mobile: 401-826-3166
PCN: 4130

From: Giles, Margaret M <Margaret.M.Giles@ice.dhs.gov>
Sent: Monday, October 28, 2019 2:43 PM
To: LaCicero, Nicole <Nicole.LaCicero@ice.dhs.gov>
Cc: Holz, Jordan <Jordan.Holz@ice.dhs.gov>; Cox, Kameron F <Kameron.F.Cox@ice.dhs.gov>
Subject: RE: Venntel - Geolocation Data Services Legal Review Process

Hi Nicole,

Alex Wood let me know that the Acting Chief Privacy Officer will be discussing this issue with the Acting General Counsel later this afternoon, and will be requesting OGC for a formal legal opinion. We should be getting more feedback from DHS OGC once that discussion happens re: next steps (and I hope/bet you will be hearing from DHS Privacy after as well).

Margaret Giles
Associate Legal Advisor
Homeland Security Investigations Law Division
Office of the Principal Legal Advisor
U.S. Immigration and Customs Enforcement
202-732-5447 (office)
202-494-0227 (mobile)
Margaret.M.Giles@ice.dhs.gov

***** WARNING *** ATTORNEY/CLIENT PRIVILEGE *** ATTORNEY WORK PRODUCT *****

This document contains confidential and/or sensitive attorney/client privileged information or attorney work product and is not for release, review, retransmission, dissemination or use by anyone other than the intended recipient. Please notify the sender if this message has been misdirected and immediately destroy all originals and copies. Any disclosure of this document must be approved by the Office of the Principal Legal Advisor, U.S. Immigration & Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY. FOIA exempt under 5 U.S.C. § 552(b)(5).

From: LaCicero, Nicole <Nicole.LaCicero@ice.dhs.gov>
Sent: Wednesday, October 23, 2019 3:57 PM
To: Giles, Margaret M <Margaret.M.Giles@ice.dhs.gov>
Cc: Holz, Jordan <Jordan.Holz@ice.dhs.gov>; Cox, Kameron F <Kameron.F.Cox@ice.dhs.gov>
Subject: Venntel - Geolocation Data Services Legal Review Process

Hi Margaret,

Have you heard from Alex Wood on whether OGC would be putting ICE's use of geolocation data through a formal legal review?

Thanks, Nicole

Nicole LaCicero, J.D./Joint M.S. Cybersecurity
Management and Program Analyst
Office of Information Governance and Privacy, Privacy Division
U.S. Immigration and Customs Enforcement
Mobile: 401-826-3166
PCN: 4130

THE MANY REVOLUTIONS OF *CARPENTER*

Paul Ohm*

TABLE OF CONTENTS

I. INTRODUCTION.....	358
II. THE NEW RULE OF <i>CARPENTER</i>	361
A. <i>Carpenter's Broad New Rule</i>	361
B. <i>On Police Efficiency and Time Machines</i>	366
C. <i>What is the Carpenter Test?</i>	369
1. First Factor: Deeply Revealing Nature.....	371
2. Second Factor: Depth, Breadth, and Comprehensive Reach.....	372
3. Third Factor: The Inescapable and Automatic Nature of the Collection.....	376
4. The Test.....	378
D. <i>Applying the Carpenter Test</i>	378
1. Very Likely Covered: Web Browsing Records.....	378
2. Most Likely Covered: Massive Collections of Telephone and Bank Records.....	381
3. Uncertain Application: Databases of Medical Records and Genetic Information	383
III. BEYOND THE CORE TEST OF <i>CARPENTER</i>	385
A. <i>Carpenter as a Replacement for Katz</i>	385
1. The Subjective Prong: <i>Katz</i> Has Only One Step	386
2. The Objective Prong: Victory of the Normative Fourth Amendment.....	387
3. The Argument for Moving Beyond <i>Katz</i>	389
B. <i>The Third-Party Doctrine, Inside Out</i>	390
C. <i>Carpenter and Direct Government Surveillance</i>	392
D. <i>The New Rule of Technological Equivalence</i>	394
1. Information from Inside the Home.....	394
2. Bailment	396
3. Private Communications	398
IV. <i>CARPENTER'S</i> TECH EXCEPTIONALISM	399
A. <i>Rejecting Conventional Analogies</i>	400

* Professor of Law and Associate Dean, Georgetown University Law Center. Thanks for excellent comments to the faculty of the University of Baltimore School of Law and the students of the law schools at Fordham and the University of Texas. Special thanks to Lindsey Barrett, Alvaro Bedoya, Steve Bellovin, Oren Bracha, Bobby Chesney, Danielle Citron, Julie Cohen, Andrew Ferguson, John Golden, Orin Kerr, Marty Lederman, and Laura Moy for comments. Thanks also to Mario Trujillo for research assistance.

<i>B. The Chief Justice's Tech Exceptionalism</i>	401
<i>C. The Argument for Tech Exceptionalism</i>	403
<i>D. Expertise and Analogy</i>	405
<i>E. Time and Technological Change</i>	408
<i>F. Refusing to Look Backwards</i>	410
1. The Surveyors	410
2. The Legal Historians	412
3. The Positive Law Proponents	413
4. Looking Forward Not Backward	413
V. CONCLUSION	415

I. INTRODUCTION

The Supreme Court's opinion in *Carpenter v. United States*¹ has been heralded by many as a milestone for the protection of privacy in an age of rapidly changing technology.² Despite this, scholars and commentators have failed to appreciate many of the important aspects of this landmark opinion. *Carpenter* works a series of revolutions in Fourth Amendment law, which are likely to guide the evolution of constitutional privacy in this country for a generation or more.

The most obvious revolution is the case's basic holding — information about the location of cell phone customers held by cell phone providers is now protected by the Fourth Amendment, at least when the police seek seven days or more of such information.³ For the first time, the Court has held that the police must secure a warrant to require a business to divulge information about its customers compiled for the business's purposes, reinventing the reasonable expectation of privacy test and significantly narrowing what is known as the third-party doctrine.⁴ This cell-site location information (“CSLI”) has become a key

1. 138 S. Ct. 2206 (2018).

2. See, e.g., Daniel Solove, *Carpenter v. United States, Cell Phone Location Records, and the Third Party Doctrine*, TEACHPRIVACY (July 1, 2018), <https://teachprivacy.com/carpenter-v-united-states-cell-phone-location-records-and-the-third-party-doctrine> [https://perma.cc/M9GD-CD6Q]; Lior Strahilevitz & Matthew Tokson, *Ten Thoughts on Today's Blockbuster Fourth Amendment Decision — Carpenter v. United States*, CONCURRING OPINIONS (June 22, 2018), <https://concurringopinions.com/archives/2018/06/ten-thoughts-on-todays-blockbuster-fourth-amendment-decision-carpenter-v-united-states.html> [https://perma.cc/Y94X-PTXR] [hereinafter Strahilevitz & Tokson, *Ten Thoughts*]; Orin Kerr, *First Thoughts on Carpenter v. United States*, REASON: THE VOLOKH CONSPIRACY (June 22, 2018, 12:20 PM), <https://reason.com/volokh/2018/06/22/first-thoughts-on-carpenter-v-united-sta> [https://perma.cc/MM3L-928T].

3. *Carpenter*, 138 S. Ct. at 2217, 2217 n.3 (“It is sufficient for our purposes today to hold that accessing seven days of [cell-site location information] constitutes a Fourth Amendment search.”).

4. *Id.* at 2221.

source of evidence for criminal investigations, so this holding will revolutionize the way the police build their cases, requiring a warrant where none has been required before.⁵

Building outward, the reasoning of the majority opinion, written by Chief Justice Roberts and commanding five votes, revolutionizes the law of police access to many other types of information, in addition to CSLI.⁶ Databases that can be used, directly or indirectly, to ascertain the precise location of individuals over time are likely now covered by the Fourth Amendment. The police will probably need a warrant to obtain location information collected by mobile apps, fitness trackers, connected cars, and many so-called “quantified self” technologies.⁷

The reasoning extends beyond location information, although predicting the scope and shape of this revolutionary step requires a bit more speculation. The majority opinion promulgates a new, multi-factor test that will likely cover other commercially significant data that the police have begun to access in its investigations.⁸ Massive databases of web browsing habits stored by internet service providers (ISPs)⁹ will probably now require a warrant to access. Perhaps most surprisingly, the majority’s reasoning will apply even to massive databases of telephone dialing and banking records, cutting back on the holdings of two cases, *Smith v. Maryland*¹⁰ and *Miller v. United States*,¹¹ that the *Carpenter* Court expressly declined to overrule.¹² Those two cases are in a much more precarious state than other commenters have recognized.¹³

Looking beyond the central holding and reasoning, to dicta from the majority and dissenting opinions, another class of revolutions comes into view. The Court has breathed new life into *Kyllo v. United States*,¹⁴ the 2001 case that required the police to obtain a warrant to aim a thermal imaging device at a private home.¹⁵ At least seven justices of the *Carpenter* Court suggest a heretofore unrecognized rule

5. *Id.* at 2233 (Kennedy, J., dissenting) (“[T]he Court’s holding . . . limits the effectiveness of an important investigative tool for solving serious crimes.”)

6. *See infra* Section III.D.

7. Andrew G. Ferguson, *The Smart Fourth Amendment*, 102 CORNELL L. REV. 547, 591–95 (2017) (discussing Fourth Amendment implications of GPS monitors attached to the body). For a discussion of these technologies, *see infra* note 51.

8. *See infra* Section II.D.

9. *See generally* Paul Ohm, *The Rise and Fall of Invasive ISP Surveillance*, 2009 U. ILL. L. REV. 1417, 1438–40 (2009), [hereinafter Ohm, *Invasive ISP Surveillance*] (describing the power of ISPs to scrutinize the private browsing habits of customers).

10. 442 U.S. 735 (1979).

11. 425 U.S. 435 (1976).

12. *Carpenter v. United States*, 138 S. Ct. 2206, 2220 (2018) (“We do not disturb the application of *Smith* and *Miller* . . .”).

13. *See, e.g.*, Solove, *supra* note 2 (“The Supreme Court should have overruled the Third Party Doctrine or at least carved out a greater chunk of it.”).

14. 533 U.S. 27 (2001).

15. *Id.* at 40.

building on *Kyllo*: the *rule of technological equivalence*. If a technology, or a near-future improvement, gives police the power to gather information that is the “modern-day equivalent” of activity that has been held to be a Fourth Amendment search, the use of that technology is also a search.¹⁶ This is a far simpler and more straightforward test to apply than the multi-factor core test of *Carpenter*, and for that reason, could end up becoming the *Carpenter* rule cited most often as the basis for requiring the police to get a warrant.

The last revolution is a revolution of legal reasoning. In his opinion, the Chief Justice evinces, as he did in the majority opinion in *Riley v. California*,¹⁷ a profound *tech exceptionalism*.¹⁸ Recent advances in information technology are different in kind, not merely in degree from what has come before. This idea finds substantial support in two decades of legal scholarship about threats from technology to information privacy, work that has never before received such a profound endorsement from the Supreme Court.

In embracing tech exceptionalism, the Court expressly declined invitations from scholars and amici to base its Fourth Amendment reasoning in traditional disciplines such as history or economics.¹⁹ Scholars coming from those interdisciplinary traditions have expressed disappointment about this choice, which is an understandable reaction to having been heard and rejected.²⁰

Carpenter is an inflection point in the history of the Fourth Amendment. From now on, we will be talking about what the Fourth Amendment means in pre-*Carpenter* and post-*Carpenter* terms. It will be considered as important as *Olmstead*²¹ and *Katz*²² in the overall arc of technological privacy.²³

This article proceeds in three parts. Part II first lays out the new rule of *Carpenter*, which protects large databases full of information from unreasonable police access according to a new, multi-factor test, and then applies the test to private databases of information beyond the one at issue in the case. Part III explains how *Carpenter* has turned the government action rule of the Fourth Amendment on its head and cre-

16. See *Carpenter*, 138 S. Ct. at 2222 (calling Justice Kennedy’s “modern-day equivalent” discussion a “sensible exception”); *id.* at 2230 (Kennedy, J., dissenting).

17. 134 S. Ct. 2473 (2014).

18. See *infra* Section IV.B.

19. See *infra* Section IV.F.

20. *Id.*

21. *Olmstead v. United States*, 277 U.S. 438 (1928) (holding that a wiretap is not a search, embracing the trespass theory of the Fourth Amendment).

22. *Katz v. United States*, 389 U.S. 347, 351 (1967) (holding that placing a recording device on the exterior of a telephone booth is a search).

23. See *infra* Section III.A.

ated three new rules of technological equivalence. Finally, Part IV discusses the tech exceptionalism at the heart of *Carpenter* and how it changes Fourth Amendment reasoning.

II. THE NEW RULE OF CARPENTER

Carpenter held that the government collection of CSLI is a search by introducing a new, multi-factor test.²⁴ This test serves the dual purpose of deciding: (1) whether access to large databases full of personal information about individuals constitutes a search under the Fourth Amendment and (2) whether the third-party doctrine should extend to such access.²⁵

The Court did not exhaustively specify or defend the new test, although a close reading of the opinion reveals the critical factors and why they matter.²⁶ When the police seek to obtain information about individual behavior contained in a private party's database, the court examines (1) "the deeply revealing nature" of the information; (2) "its depth, breadth, and comprehensive reach"; and (3) "the inescapable and automatic nature of its collection."²⁷ The importance of these factors finds great support in recent legal scholarship.²⁸ When lower courts apply these factors, they are likely to extend the Fourth Amendment to cover many important commercial databases that have never before required a warrant for the police to access.

A. *Carpenter's Broad New Rule*²⁹

Carpenter held that the police may not collect historical CSLI from a cell phone service provider without a warrant.³⁰ Footnote three restricted the holding, for now, to seven days of collection.³¹

24. *Carpenter v. United States*, 138 S. Ct. 2206, 2223 ("In light of the deeply revealing nature of CSLI, its depth, breadth, and comprehensive reach, and the inescapable and automatic nature of its collection, the fact that such information is gathered by a third party does not make it any less deserving of Fourth Amendment protection.").

25. *See id.*

26. *See infra* Section II.C.

27. *Carpenter*, 138 S. Ct. at 2223 (emphasis added).

28. *See infra* Section III.C (connecting each of the *Carpenter* factors to recent legal scholarship).

29. This subpart is adapted from a blog post I authored shortly after the *Carpenter* decision was handed down. *See* Paul Ohm, *The Broad Reach of Carpenter v. United States*, JUST SECURITY (June 27, 2018), <https://www.justsecurity.org/58520/broad-reach-carpenter-v-united-states> [https://perma.cc/2FL2-KPSS].

30. *Carpenter*, 138 S. Ct. at 2217.

31. *Id.* at 2217 n.3.

This is the opinion most privacy law scholars and privacy advocates have been awaiting for decades.³² Oceans of ink have been spilled by those worried about how the dramatic expansion of technologically fueled corporate surveillance of our private lives automatically expands police surveillance too, thanks to the way the Supreme Court has construed the reasonable expectation of privacy test and the third-party doctrine.³³ The Fourth Amendment protects only that which is protected by a “reasonable expectation of privacy” (“REP”).³⁴ This requires a two-pronged analysis, “first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as ‘reasonable.’”³⁵ The third-party doctrine says that information a person voluntarily discloses to a third party is not protected by a reasonable expectation of privacy.³⁶

With *Carpenter*, the Supreme Court reinvents the REP test. Until now, the Supreme Court has tended to pay more attention to the nature of the police intrusion required to obtain information than to the nature of the information obtained. Information has been deemed protected by REP because the police obtained it using advanced thermal imaging tools,³⁷ or a wireless beeper located inside a house.³⁸ Information has

32. DAVID GRAY, *THE FOURTH AMENDMENT IN AN AGE OF SURVEILLANCE* 17 (2017) (“The task for the Court in our age of surveillance is to fashion new Fourth Amendment remedies to meet twenty-first-century challenges.”); DANIEL J. SOLOVE, *NOTHING TO HIDE: THE FALSE TRADEOFF BETWEEN PRIVACY AND SECURITY* 2 (2011) (“When evaluating security measures, judges are often too deferential to security officials. And the law gets caught up in cumbersome tests to determine whether government information gathering should be subjected to oversight and regulation, resulting in uneven and incoherent protection.”); Susan Freiwald, *Cell Phone Location Data and the Fourth Amendment: A Question of Law, Not Fact*, 70 MD. L. REV. 681, 746 (2011) (advocating for judicial determination that individuals have an objectively reasonable expectation of privacy in location information) [hereinafter Freiwald, *Cell Phone Location Data*].

33. See, e.g., Susan Freiwald, *First Principles of Communications Privacy*, 2007 STAN. TECH. L. REV. 3 at *49 (2007) (“By focusing merely on whether third parties have access to our communications data, or whether that data can be characterized as non-contents, courts have authorized increasingly powerful surveillance methods without meaningful judicial oversight.”) [hereinafter Freiwald, *First Principles*]; David Gray & Danielle Citron, *The Right to Quantitative Privacy*, 98 MINN. L. REV. 62, 139–40 (2013) (“The implications for Fourth Amendment interests in quantitative privacy are obvious. What the government cannot collect or aggregate directly, it can simply get from third parties with whom the information has been shared.”); Neil Richards, *The Third-Party Doctrine and the Future of the Cloud*, 94 WASH. U.L. REV. 1441, 1482 (2017) (“If we accept the logic of the Third-Party Doctrine for our current data practices, then it would logically follow that future data sets would also lose Fourth Amendment protection.”).

34. *Katz v. United States*, 389 U.S. 347, 360–61 (1967) (Harlan, J., concurring) (articulating the reasonable expectation of privacy test).

35. *Id.*

36. See Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 566–70 (2009).

37. *Kyllo v. United States*, 533 U.S. 27, 34–35 (2001).

38. *United States v. Karo*, 468 U.S. 705, 714–15 (1984).

fallen outside an REP when obtained from trash left on the curb,³⁹ low-flying aircraft,⁴⁰ or a wireless beeper traveling on public roads.⁴¹ The analysis has almost always turned primarily on the invasion and only secondarily on the information.

Carpenter heralds a new mode of Constitutional analysis because the Court finds an REP based largely on an analysis of the information divorced from the actions of the police, database owner, or surveillance target. The most important holding — which commanded the votes of five justices — is that “individuals have a reasonable expectation of privacy in the whole of their physical movements.”⁴² The Court explains that a database full of CSLI meets this standard using an analysis focused exclusively on the nature of the data in the database and the target’s role in its initial collection.

Next, with *Carpenter*, the third-party doctrine appears to be nearly dead. The majority opinion “decline[d] to extend” the third-party doctrine to the FBI’s collection of seven days of CSLI from cell phone service providers.⁴³ “Given the unique nature of cell phone location information, the fact that the Government obtained the information from a third party does not overcome *Carpenter*’s claim to Fourth Amendment protection.”⁴⁴

Even on their own terms, these two holdings have sweeping consequences for privacy and law enforcement. But it is the manner in which Chief Justice Roberts reasoned his way to them that assures that this opinion will be applied far beyond the facts of this case.

First, as described in the majority and dissenting opinions, the CSLI that has just been protected is not terribly precise.⁴⁵ If the majority had placed an exaggerated gloss on the precision of CSLI at issue in this case, it would have given the government a way in future cases to distinguish other types of location information: “the data at issue in this case is not controlled by *Carpenter*,” the government could have argued, “because it is far less precise than CSLI.”

But, it will be difficult to make this argument because the majority opinion informs us that the CSLI records in this case “placed [*Carpenter*] within a wedge-shaped sector ranging from one-eighth to four square miles.”⁴⁶ In his dissent, Justice Kennedy characterized these dimensions as “covering between a dozen and several hundred city

39. *California v. Greenwood*, 486 U.S. 35, 40 (1988).

40. *Florida v. Riley*, 488 U.S. 445, 450 (1989).

41. *United States v. Knotts*, 460 U.S. 276, 281–82 (1983).

42. *Carpenter v. United States*, 138 S. Ct. 2206, 2217 (citing *United States v. Jones*, 565 U.S. 400, 430 (2012) (Alito, J., concurring); *id.* at 415 (Sotomayor, J., concurring)).

43. *Carpenter*, 138 S. Ct. at 2220.

44. *Id.*

45. *Id.* at 2218.

46. *Id.*

blocks” in cities and “up to 40 times more imprecise” in rural areas.⁴⁷ GPS this certainly is not. The Chief Justice waves this away, in part, because “the rule this Court adopts ‘must take account of more sophisticated systems that are already in use or in development.’”⁴⁸

Second, the majority opinion is not restricted to CSLI. Instead, this is an opinion about information the police can use to locate people generally, not CSLI specifically.⁴⁹ Part IV of the opinion is all about the privacy interests individuals have in “the whole of their physical movements.”⁵⁰ This is a meditation on the nature of location information, whatever form it takes. Geolocation information, when there is enough of it, “provides an intimate window into a person’s life,” quoting Justice Sotomayor’s celebrated opinion from *Jones*, revealing “familial, political, professional, religious, and sexual associations.”⁵¹ This case is “not about ‘using a phone’ . . . [i]t is about a detailed chronicle of a person’s physical presence compiled every day, every moment, over several years.”⁵² It is about “a trail of location data.”⁵³

By focusing on the nature of the information rather than on the telecommunications nitty-gritty used to gather the information or the structure of the database in which the information was held, this opinion provides analysis that should apply to other massive collections of historical geolocation information, of which there are many. Many smartphone apps collect precise GPS information, including apps that have no need for this kind of information except to sell to advertisers.⁵⁴ It is not just your smartphone, as GPS information is gathered by the companies that provide fitness trackers, connected cars, and smart watches. Internet of Things gizmos can place location trackers on our clothes, bags, and even our bodies.⁵⁵ It might not be that every database

47. *Id.* at 2225 (Kennedy, J., dissenting).

48. *Id.* at 2218–19 (quoting *Kyllo v. United States*, 533 U.S. 27, 36 (2001)).

49. *Id.* at 2217–18.

50. *Id.* at 2217 (citing *United States v. Jones*, 565 U.S. 400, 430 (2012) (Alito, J., concurring); *id.* at 415 (Sotomayor, J., concurring)).

51. *Carpenter*, 138 S. Ct. at 2217 (quoting *United States v. Jones*, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring)).

52. *Id.* at 2220.

53. *Id.*

54. See, e.g., KENNETH OLMSTEAD & MICHELLE ATKINSON, PEW RESEARCH CENTER, APP PERMISSIONS IN THE GOOGLE PLAY STORE 22 (2015), http://assets.pewresearch.org/wp-content/uploads/sites/14/2015/11/PI_2015-11-10_apps-permissions_FINAL.pdf [<https://perma.cc/GQ3Y-RPP2>] (finding that in 2014, 24% of apps in the Google Play store requested access to precise GPS location information, while 21% asked for approximate location information); Press Release, Fed. Trade Comm’n, Android Flashlight App Developer Settles FTC Charges It Deceived Consumers (Dec. 5, 2013), <https://www.ftc.gov/news-events/press-releases/2013/12/android-flashlight-app-developer-settles-ftc-charges-it-deceived> [<https://perma.cc/TX29-JZAQ>] (announcing settlement of case against flashlight app manufacturer for sharing precise geolocation information with third parties, thwarting consumer expectations).

55. See, e.g., OFFICE OF SEN. ED MARKEY, TRACKING & HACKING: SECURITY & PRIVACY GAPS PUT AMERICAN DRIVERS AT RISK 8 (2015), <https://www.markey.senate.gov/imo/>

of location information generated by every technology listed above will fall within the *Carpenter* reasoning, but the police should think twice before trying to collect any of it without a warrant.

Third, the majority opinion will probably even apply to information that does not expressly reveal location but from which location may be inferred. “[T]he Court has already rejected the proposition that ‘inference insulates a search,’”⁵⁶ quoting *Kyllo* once again. The opinion highlights how the government could use CSLI “in combination with other information, [to] deduce a detailed log of Carpenter’s movements.”⁵⁷ Many databases that do not store location information directly can be used to infer location information. Credit card records, automatic toll transponder records, automated license-plate records, etc., can all generate inferences about a person’s location that are far more precise than CSLI.⁵⁸ Any time the government accesses a privately assembled database in order to track location over time without a warrant, it risks suppression under *Carpenter*.

media/doc/2015-02-06_MarkeyReport-Tracking_Hacking_CarSecurity%202.pdf [https://perma.cc/4VQH-22GE] (describing collection and transmission of driving history from connected cars); Damon Beres, *These High-Tech Shirts And Pants Can Help Protect Kids With Autism*, THE HUFFINGTON POST (last updated Dec. 6, 2017), https://www.huffingtonpost.com/2015/02/18/autism-gps-device_n_6705368.html [https://perma.cc/4VQH-22GE] (describing location tracking in clothing for autistic children); Carey Dunne, *Forget Fitbits: This T-Shirt Embeds Fitness Sensors Into Its Fabric*, FAST COMPANY (Mar. 6, 2014), https://www.fastcompany.com/3027278/forget-fitbits-this-t-shirt-embeds-fitness-sensors-into-its-fabric [https://perma.cc/GLN8-4B4K] (describing location tracking in exercise clothing); Lisa Eadicicco, *A New Wave Of Gadgets Can Collect Your Personal Information Like Never Before*, BUS. INSIDER (Oct. 9, 2014, 11:26 AM), https://www.businessinsider.com/privacy-fitness-trackers-smartwatches-2014-10 [https://perma.cc/J2Q3-ZTZ7] (describing location tracking in smartwatches and fitness trackers); Ferguson, *The Smart Fourth Amendment*, *supra* note 7 (discussing Fourth Amendment implications of GPS monitors attached to the body); Melanie Swan, *Sensor Mania! The Internet of Things, Wearable Computing, Objective Metrics, and the Quantified Self 2.0*, 1 J. SENSOR & ACTUATOR NETWORKS 217, 221 (2012) (describing GPS monitoring in at least one wristband sensor). Cf. Yael Grauer, *A practical guide to microchip implants*, ARS TECHNICA (Jan. 3, 2018, 7:30 AM), https://arstechnica.com/features/2018/01/a-practical-guide-to-microchip-implants [https://perma.cc/QAG6-YBKB] (describing transponder implants in humans but not referring to GPS).

56. *Carpenter*, 138 S. Ct. at 2218 (quoting *Kyllo v. United States*, 533 U.S. 27, 36 (2001)).

57. *Id.*

58. *See, e.g.*, *United States v. Kragness*, 830 F.2d 842, 865 (8th Cir. 1987) (describing government’s use of credit-card records to prove defendant’s travel history); *In re U.S. for Historical Cell Site Data*, 724 F.3d 600, 614 n.13 (5th Cir. 2013) (“[W]hen a customer makes a credit card purchase at a store or restaurant, he does not directly convey the location of the transaction to his credit card company. Nevertheless, law enforcement officers can obtain his credit card records from the company with a subpoena . . . and use them to track his location . . .”); Mariko Hirose, *Newly Obtained Records Reveal Extensive Monitoring of E-ZPass Tags Throughout New York*, AM. CIVIL LIBERTIES UNION (Apr. 24, 2015, 1:00 PM), https://www.aclu.org/blog/privacy-technology/location-tracking/newly-obtained-records-reveal-extensive-monitoring-e-zpass [https://perma.cc/3BXX-5N7Z] (describing location tracking through toll transponders); Reepal S. Dalal, Note, *Chipping away at the Constitution: The Increasing Use of RFID Chips Could Lead to an Erosion of Privacy Rights*, 86 B.U. L. REV. 485, 494–95 (2006) (discussing the Fourth Amendment implications of toll collection data); AM. CIVIL LIBERTIES UNION, YOU ARE BEING TRACKED: HOW LICENSE PLATE READERS ARE BEING USED TO RECORD AMERICANS’ MOVEMENTS 7 (2013),

This gives the lie to something the majority said that has puzzled commenters: “We do not . . . call into question conventional surveillance techniques and tools, such as security cameras.”⁵⁹ What the Chief Justice misses in this simple statement is how facial recognition technology has advanced to the point that a huge archive of security camera footage can easily be transformed into a massive database tracking the location of identified individuals.⁶⁰ It might be that CSLI records track location far more comprehensively than security camera footage connected to facial recognition software — we will examine the role of the comprehensiveness below⁶¹ — but the majority cannot literally mean that security camera footage is categorically not a search given the reasoning of the opinion.

In sum, criminal defendants will test the outer boundaries of *Carpenter*’s reasoning whenever the police use massive databases assembled by private parties that reveal location information, directly or by inference. Other defendants will challenge the collection of data unrelated to location. The broad reasoning of the majority’s opinion will give all of them plenty to work with. Anticipating this, risk-averse police departments will err on the side of caution, getting a warrant for data whenever they can, sometimes turning promising leads into dead ends. It’s a powerful reminder of the ability the Supreme Court has to protect civil liberties and reshape the contours of our relationship with the state.

B. On Police Efficiency and Time Machines

At the outset of his opinion, the Chief Justice frames two overarching purposes for the Fourth Amendment: “to secure ‘the privacies of life’ against ‘arbitrary power’” and “to place obstacles in the way of a too permeating police surveillance.”⁶² The majority’s opinion is centrally preoccupied with the way technology has made the police more efficient. The opinion returns repeatedly to the idea that this increased efficiency has Fourth Amendment import.

<https://www.aclu.org/files/assets/071613-aclu-alprreport-opt-v05.pdf> (describing location tracking through license-plate records) [<https://perma.cc/2ANN-4654>]; *infra* note 212 (discussing Fourth Amendment implications of license plate readers).

59. *Carpenter*, 138 S. Ct. at 2220.

60. GARVIE ET AL., THE PERPETUAL LINE-UP: UNREGULATED POLICE FACE RECOGNITION IN AMERICA 22 (2016), <https://www.perpetuallineup.org/sites/default/files/2016-12/The%20Perpetual%20Line-Up%20-%20Center%20on%20Privacy%20and%20Technology%20at%20Georgetown%20Law%20-%2020121616.pdf> [<https://perma.cc/5K99-H27P>] (“describing facial recognition software used by law enforcement agencies for purposes including geolocation”).

61. *Infra* Section II.C.

62. *Carpenter*, 138 S. Ct. at 2214 (first quoting *Boyd v. United States*, 116 U.S. 616, 630 (1886); and then quoting *United States v. Di Re*, 332 U.S. 581, 595 (1948)).

The idea of police efficiency is given one particularly evocative and salient analogy: crime fighting time machines. A key distinction between CSLI and other location tracking methods from history is the fact that with CSLI, everyone is being tracked at all times, long before any one of us falls under the scrutiny of the police. The metaphor of police access to historical data as time travel was first proposed by legal scholar Stephen Henderson.⁶³

There are, however, two ways to read this attention to police efficiency gain: First, this might be what connects the *Carpenter* holding to *Katz*. Members of society do not expect the gains in efficiency of the police, and it is this misalignment in our expectations that leads to the conclusion that a search has occurred:

Prior to the digital age, law enforcement might have pursued a suspect for a brief stretch, but doing so “for any extended period of time was difficult and costly and therefore rarely undertaken.” For that reason, “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.” . . . And like GPS monitoring, cell phone tracking is remarkably easy, cheap, and efficient compared to traditional investigative tools. With just the click of a button, the Government can access each carrier’s deep repository of historical location information at practically no expense.⁶⁴

The two internal quotes come from Justice Alito’s concurrence in *Jones*, which also placed great weight on preventing the power of the police to increase dramatically through the progress of technology.⁶⁵

The second way to read the *Carpenter* court’s focus on increased police efficiency treats the Fourth Amendment as a constitutional lever. This interpretation can require the police to be more inefficient than modern technology would otherwise allow, by forcing the police to stop and get a warrant. The court, quite strikingly, recited near the very beginning of its discussion of the doctrine that a “central aim of the Framers was ‘to place obstacles in the way of a too permeating police surveillance.’”⁶⁶

63. Stephen E. Henderson, *Fourth Amendment Time Machines (and What They Might Say About Police Body Cameras)*, 18 U. PENN. J. CON. L. 933, 935 (2016).

64. *Carpenter*, 138 S. Ct. at 2217–18 (internal citations omitted).

65. *United States v. Jones*, 565 U.S. 400, 429–430 (2012) (Alito, J., concurring).

66. *Carpenter*, 138 S. Ct. at 2214.

There is a subtle but important difference in these two approaches. The former is a less interventionist, more reactive role for the judiciary going forward: the judge's role is to note those moments when public expectation diverges from technological reality and to temporarily slow things down. Presumably, at some point society's expectations will catch up to the technologically possible; at some point we will recognize that we live in an age of technologically abetted super police. At that moment, the passive approach would suggest, we can dispense with the warrant requirement in this case.

In contrast, the latter assigns a far more interventionist and proactive role for judges. As stated in *Carpenter* above, the role of judges is to "place obstacles in the way of a too permeating police surveillance." This suggests a much more long-lived state of affairs. Warrants are required to add friction in the way of our technologically abetted super police. Even if society begins to expect a more efficient police force, the police will still be required to subject itself to the twin ordeals of probable cause and judicial review.

To put it more colloquially, the former approach is like a speed bump, while the latter is like a road block. In either event, *Carpenter* puts to rest the dictum in *United States v. Knotts*⁶⁷ that "[w]e have never equated police efficiency with unconstitutionality, and we decline to do so now."⁶⁸

Time — and further case law development — will tell which of these interpretations controls after *Carpenter*. I prefer the more interventionist version: the Fourth Amendment should be seen as a road-block to a hyper-efficient police force. It should require warrants not only until society grows accustomed to powerful new forms of surveillance; warrant requirements must have a more lasting and durable lifespan. The interventionist interpretation also finds support from a broad range of legal scholarship.⁶⁹ Of most direct relevance, it stems from an important article by Kevin Bankston and Ashkan Soltani.⁷⁰ They argue that the police engage in a Fourth Amendment search whenever a new technology makes it "much less expensive" to collect information about individuals.⁷¹ The article presents a compelling case that the facts of *Jones* meets this standard, because a police-installed GPS

67. *United States v. Knotts*, 460 U.S. 276 (1983).

68. *Id.* at 284.

69. See, e.g., Luke M. Milligan, *Analogy Breakers: A Reality Check on Emerging Technologies*, 80 MISS. L.J. 1319, 1337 (2011) (arguing that the increased efficiency of the government should be a factor in considering whether a court should engage in a "fresh" analysis of a legal doctrine).

70. Kevin S. Bankston & Ashkan Soltani, *Tiny Constables and the Cost of Surveillance: Making Cents Out of United States v. Jones*, 123 YALE L.J. ONLINE 335 (2014), <http://yalelawjournal.org/forum/tiny-constables-and-the-cost-of-surveillance-making-cents-out-of-united-states-v-jones> [<https://perma.cc/NBL9-PN59>].

71. *Id.* at 337.

tracker significantly reduces the cost of location tracking. They lend rigor to this conclusion by meticulously reading FBI pursuit manuals and cross-referencing them to FBI Special Agent salary tables to conclude that a GPS tracker is twenty-eight times cheaper than covert pursuit, while tracking location by cell phone — akin to the facts of *Carpenter* — is almost twice as cheap as GPS tracking.⁷²

Bankston and Soltani pay due to other scholarship, most importantly Orin Kerr's theory of equilibrium adjustment.⁷³ According to this influential theory, "[w]hen new tools and new practices threaten to expand or contract police power in a significant way, courts adjust the level of Fourth Amendment protection to try to restore the prior equilibrium."⁷⁴ *Carpenter* is the ultimate embrace of both the Bankston-Soltani theory of efficiency and the Kerr theory of equilibrium adjustment.⁷⁵

Whether the Court intended the weaker or stronger approach to responding to police efficiency will dictate how long we will be governed by particular warrant requirements. But at least in the short term, what emerges is the same three-factor test.

C. What is the Carpenter Test?

The test that emerges from the majority opinion will also be applied to collections of information maintained by third parties that do not track location, not even by inference, but are of interest to law enforcement. Going forward, whenever the government obtains a copy of a massive database of information containing non-public information about individuals, judges will conduct a qualitative and quantitative assessment of the information, using a new, multi-factor test. This assessment will answer two questions: First, does the individual whose information has been obtained have a reasonable expectation of privacy in the database? Second, even if that information has been collected and

72. *Id.* at 354 (depicting visually the efficiency multipliers of using technology to track location as opposed to manual surveillance).

73. *Id.* at 337–38 n.10 (citing Orin S. Kerr, *An Equilibrium-Adjustment Theory of the Fourth Amendment*, 125 HARV. L. REV. 476 (2011) [hereinafter Kerr, *Equilibrium*]). They also generously connect it to my earlier writing. *Id.* at 337 n.11 (citing Paul Ohm, *The Fourth Amendment in a World Without Privacy*, 81 MISS. L.J. 1309, 1312 (2012)). The final building block is the work of Harry Surden, *Structural Rights in Privacy*, 60 SMU L. REV. 1605 (2007).

74. Kerr, *Equilibrium*, *supra* note 73, at 480.

75. See Orin Kerr, *Understanding the Supreme Court's Carpenter Decision*, LAWFARE (June 22, 2018, 1:18 PM), <https://www.lawfareblog.com/understanding-supreme-courts-carpenter-decision> [<https://perma.cc/A4LD-5V8K>] (arguing that the majority opinion embraces equilibrium-adjustment theory). No less than Edward Snowden has embraced this reading. Edward Snowden (@Snowden), TWITTER (June 22, 2018, 9:23 AM), <https://twitter.com/Snowden/status/1010196684066959360> [<https://perma.cc/9C24-8GJY>] ("The Bankston-Soltani Principle is alive and well.").

is being maintained by a private third party, does the third-party doctrine apply?

There is likely to be disagreement about the precise list of *Carpenter* factors, given the wide-ranging nature of the opinion. Different characteristics of CSLI data and smartphone use are emphasized throughout Chief Justice Roberts's opinion.⁷⁶ Still, in concluding the opinion, he helpfully isolates three factors: (1) "the deeply revealing nature" of the information; (2) "its depth, breadth, and comprehensive reach"; and (3) "the inescapable and automatic nature of its collection."⁷⁷

Later, I will say even more about the theoretical foundations and normative desirability of this test,⁷⁸ but for now, let us note the similarity of the test to the work of Susan Freiwald.⁷⁹ Freiwald has long advocated that the Court embrace her own four-factor test for deciding whether there is an invasion of REP in electronic surveillance.⁸⁰ She argues that courts should inquire whether the police are using a "hidden, intrusive, indiscriminate, and continuous method of surveillance."⁸¹ Using this test, she bested the Supreme Court by seven years, arguing in 2011 that the police should be required to obtain a warrant to access CSLI.⁸²

Let us consider each of the *Carpenter* factors in turn. The sections that follow will highlight the key language from the majority opinion about each factor, as well as focus on language from the various dissents that sharpen the meaning or import of each factor. These sections will also connect most of the factors to the broader world of privacy law and scholarship beyond this case. This is meant to address a criticism that has been directed at the majority's opinion: its failure to cite any legal scholarship.⁸³ The Court could have supported each of its points with scholarly citation. However, this opinion still resonates with two decades of writing about the Fourth Amendment in an age of rapidly changing technology, regardless of whether the Chief Justice was aware of any of this work. Consider this the majority's missing cite check, demonstrating the rigor and theoretical underpinnings of this approach.

76. *Carpenter v. United States*, 138 S. Ct. 2206, 2216–20 (2018).

77. *Id.* at 2223.

78. See *infra* Parts III–IV.

79. See Susan Freiwald, *Cell Phone Location Data and the Fourth Amendment: A Question of Law, Not Fact*, 70 MD. L. REV. 681, 746 (2011) [hereinafter Freiwald, *Cell Phone Location Data*]; Freiwald, *First Principles*, *supra* note 33.

80. Freiwald, *First Principles*, *supra* note 33; *infra* Section IV.B (explaining and defending the four-factor test).

81. Freiwald, *First Principles*, *supra* note 33 at *50.

82. Freiwald, *Cell Phone Location Data*, *supra* note 79, at 746–48.

83. See, e.g., Strahilevitz & Tokson, *Ten Thoughts*, *supra* note 2.

1. First Factor: Deeply Revealing Nature

The *Carpenter* test protects information only if it is “deeply revealing” of some private quality of the person under surveillance.⁸⁴ “As with GPS information, the time-stamped data provides an intimate window into a person’s life, revealing not only his particular movements, but through them his ‘familial, political, professional, religious, and sexual associations.’”⁸⁵ These location records ‘hold for many Americans the privacies of life.’”⁸⁶

To give labels to these requirements, information stored by a private third party must in some way be deemed sensitive or intimate to fall within the reasonable expectation of privacy test. These two words, although similar to one another, have different meanings. Sensitive information is information that can be used to cause an individual or group harm.⁸⁷ In contrast, intimate information reveals something important and not widely known about a relationship between individuals.⁸⁸

The connection between sensitive and intimate information and the REP test has a long doctrinal lineage. Professor Orin Kerr argues that the Supreme Court has adopted four different models for assessing whether police practice implicates a reasonable expectation of privacy, one of which is a “private facts” model. This model measures the sensitivity and intimacy of the information obtained.⁸⁹

The road to the Court’s recognition of the “deeply revealing nature” factor was paved by the two blockbuster opinions from recent years about technology and the Fourth Amendment, *United States v. Jones* and *Riley v. California*.⁹⁰ The notion that detailed location information can reveal one’s “familial, political, professional, religious, and sexual associations” comes from Justice Sotomayor’s concurrence in *Jones*,⁹¹ perhaps the single most important quote ever uttered in a Supreme Court opinion about the sensitivity of information. The idea that a smart phone can “hold for many Americans, the ‘privacies of life’” comes from Chief Justice Roberts’s opinion in *Riley*.⁹²

84. *Carpenter v. United States*, 138 S. Ct. 2206, 2223 (2018).

85. *Id.* at 2217 (quoting *United States v. Jones*, 565 U.S. 400, 415 (2012)) (citations and internal quotation marks omitted).

86. *Id.* (quoting *Riley v. California*, 134 S. Ct. 2473, 2495 (2014)) (citations and internal quotation marks omitted).

87. See Paul Ohm, *Sensitive Information*, 88 S. CAL. L. REV. 1125, 1133–34 (2015) [hereinafter Ohm, *Sensitive Information*].

88. See JULIE C. INNESS, *PRIVACY, INTIMACY, AND ISOLATION* 56–57 (1992).

89. Orin S. Kerr, *Four Models of Fourth Amendment Protection*, 60 STAN. L. REV. 503, 512–15 (2007) [hereinafter Kerr, *Four Models*]. The other three models are “probabilistic,” “positive law,” and “policy.” *Id.* at 506. We will return to this later.

90. 565 U.S. 400 (2012); 134 S. Ct. 2473 (2014).

91. *Jones*, 565 U.S. at 415 (Sotomayor, J., concurring).

92. *Riley*, 134 S. Ct. at 2494–95 (quoting *Boyd v. United States*, 116 U.S. 616, 630 (1886)).

As discussed earlier, this factor focuses exclusively on an analysis of the intrinsic nature of the information itself, divorced from any consideration of what the police had to do to obtain it, the company's incentives for gathering it, or what the individual could have done to prevent it. *Carpenter* is a fundamental break from most Fourth Amendment analyses of the past, which almost always placed police action and individual counter-action at the center, and information on the periphery.

2. Second Factor: Depth, Breadth, and Comprehensive Reach

The *Carpenter* test protects information that possesses “depth, breadth, and comprehensive reach.”⁹³ Like the first factor, the second factor focuses on the intrinsic nature of the information.

Justice Kennedy, in dissent, provided his own list of the factors he saw in the majority's opinion, to criticize the majority's “unstable foundation.”⁹⁴ Of the factors in his list, the one that most closely resembles “depth, breadth, and comprehensive reach” is a single factor, “comprehensiveness,”⁹⁵ but it is better to treat this as comprising three distinct requirements (meaning our three factors might instead be treated as five). All three primarily speak to the quantity of information stored. But they measure a database along three distinct dimensions.

Depth refers to the detail and precision of the information stored.⁹⁶ This is closely related to the deeply revealing nature factor, as it is the precision of location information that triggers Justice Sotomayor's litany of private inferences — location information betrays a person's “familial, political, professional, sexual, religious, and sexual associations” only if it is sufficiently precise to imply visits to particular storefronts, homes, or other individual locations.⁹⁷ The *Carpenter* majority emphasizes that CSLI stores “the whole of [a person's] physical movements”⁹⁸ as well as “a detailed chronicle of a person's physical presence.”⁹⁹

In contrast, *breadth* refers to time in two ways: how frequently the data is collected, and for how long the data has been recorded.¹⁰⁰ CSLI

93. *Carpenter v. United States*, 138 S. Ct. 2206, 2223 (2018).

94. *Id.* at 2234 (Kennedy, J., dissenting).

95. *Id.*

96. *See id.* at 2218 (majority opinion) (“From the 127 days of location data it received, the Government could, in combination with other information, deduce a detailed log of Carpenter's movements, including when he was at the site of the robberies. And the Government thought the CSLI accurate enough to highlight it during the closing argument of his trial.”).

97. *Id.* at 2217 (quoting *United States v. Jones*, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring)).

98. *Id.* at 2219.

99. *Id.* at 2220.

100. *See id.* at 2212 (“Altogether the Government obtained 12,898 location points cataloging Carpenter's movements — an average of 101 data points per day.”).

qualifies as broad in both senses, because the database at issue in *Carpenter* stored “an average of 101 data points per day” of the defendant’s location,¹⁰¹ and because cell phone providers tend to store data for up to five years.¹⁰² Every one of us “has effectively been tailed every moment of every day for five years.”¹⁰³ It is information “compiled every day, every moment, over several years.”¹⁰⁴

Finally, *comprehensive reach* refers to the number of people tracked in the database.¹⁰⁵ This recognizes that there, but by the grace of the police, go I. “Critically, because location information is continually logged for all of the 400 million devices in the United States — not just those belonging to persons who might happen to come under investigation — this newfound tracking capacity runs against everyone.”¹⁰⁶ This is critical because, “[u]nlike with the GPS device in *Jones*, police need not even know in advance whether they want to follow a particular individual, or when.”¹⁰⁷ By identifying these factors in *Carpenter*, the Court in effect endorses the mosaic theory of privacy.¹⁰⁸ The mosaic theory is animated by an idea that finds support both in folk wisdom and modern machine learning: the whole is greater than the sum of the parts.¹⁰⁹ It first found expression in Fourth Amendment jurisprudence in *United States v. Maynard*,¹¹⁰ the D.C. Circuit opinion that was renamed *United States v. Jones* on its way to the Supreme Court. In the majority opinion in *Maynard*, Judge Ginsburg concluded that “[p]rolonged 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.”¹¹¹ Although the *Jones* majority chose not to embrace the mosaic theory, focusing instead on the physical trespass that occurred during the installation of the GPS tracking device,¹¹² *Carpenter* seems to revive the idea.

101. *Id.*

102. *Id.* at 2218.

103. *Id.*

104. *Id.* at 2220.

105. *See id.* at 2218 (“Whoever the suspect turns out to be, he has effectively been tailed every moment of every day for five years, and the police may — in the Government’s view — call upon the results of that surveillance without regard to the constraints of the Fourth Amendment. Only the few without cell phones could escape this tireless and absolute surveillance.”).

106. *Id.*

107. *Id.*

108. *See* Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311, 313–14 (2012) [hereinafter Kerr, *Mosaic Theory*] (defining “mosaic theory” of privacy).

109. *Id.* at 326.

110. 615 F.3d 544 (D.C. Cir. 2010), *aff’d sub nom.* *United States v. Jones*, 565 U.S. 400 (2012).

111. *Id.* at 562.

112. *United States v. Jones*, 565 U.S. 400, 404 (2012).

The mosaic theory brings us to footnote three of *Carpenter*:

The parties suggest as an alternative to their primary submissions that the acquisition of CSLI becomes a search only if it extends beyond a limited period. As part of its argument, the Government treats the seven days of CSLI requested from Sprint as the pertinent period, even though Sprint produced only two days of records. Contrary to Justice KENNEDY's assertion, we need not decide whether there is a limited period for which the Government may obtain an individual's historical CSLI free from Fourth Amendment scrutiny, and if so, how long that period might be. It is sufficient for our purposes today to hold that accessing seven days of CSLI constitutes a Fourth Amendment search.¹¹³

Two of the dissents criticized the seeming arbitrariness of this seven-day rule.¹¹⁴ Footnote three has already sparked scholarly criticism and commentary.¹¹⁵ Any opinion that tries to give force to the mosaic theory has to draw a line.¹¹⁶ Given the role that the quantity factors play in the majority's reasoning, it seems likely that a database containing a single datum that revealed a single registration between a cell phone and cell site would not trigger nearly the same privacy concerns. A single data point would be neither as deep, broad, nor comprehensive, as seven days (much less five years) of CSLI. For that reason, it would not be nearly as "deeply revealing." A future court asked to rule on the warrantless access of a single datum of location information might well distinguish it from the facts and reasoning of *Carpenter*.

While one point of information might not suffice, one should not read too much into the seven-day figure. For one thing, this is the figure that the facts presented: the government sought seven days of CSLI.¹¹⁷ In fact, the order seeking seven days of information elicited only two days of CSLI.¹¹⁸ The Court gave no principled reason for selecting

113. *Carpenter v. United States*, 138 S. Ct. 2206, 2217 n.3 (2018) (citations omitted).

114. *Id.* at 2234 (Kennedy, J., dissenting); *id.* at 2266–67 (Gorsuch, J., dissenting).

115. See, e.g., ORIN S. KERR, *THE DIGITAL FOURTH AMENDMENT* (forthcoming 2019) [hereinafter KERR, *DIGITAL FOURTH AMENDMENT*]; Susan Freiwald & Stephen Wm. Smith, *The Carpenter Chronicle: A Near-Perfect Surveillance*, 132 HARV. L. REV. 205, 228 (2018).

116. Kerr, *Mosaic Theory*, *supra* note 108, at 333–34 (discussing the need to draw lines based on time for a mosaic theory approach to the Fourth Amendment).

117. *Carpenter*, 138 S. Ct. at 2212; see also *id.* at 2217 n.3 (citing the government's suggestion of a seven-day cutoff for CSLI acquisition to become a search).

118. *Id.* at 2212.

seven days as the cut-off, so we ought not consider it the precise dividing line. Future opinions will need to analyze the relationship between the temporal breadth of data and the impact on privacy interests.

These quantitative facts are sure to be the source of confusion in the lower courts — and inside police stations — and the target of criticism from other scholars.¹¹⁹ What if a database has only two forms of quantitative comprehensiveness — say depth and breadth — but about only one person, rather than with comprehensive reach? What if a database reveals deep information about many people, but recorded at a single moment in time?

One potential complicating scenario was expressly referenced in the majority opinion: Does a real-time, future-looking, prospective collection of data trigger this factor and thus the *Carpenter* rule?¹²⁰ The majority opinion expressly declined to say.¹²¹ At the same time, it emphasized repeatedly the retrospective nature of CSLI information, and indeed, Justice Kennedy included “retrospectivity” in his summary of the factors, although the majority opinion did not.¹²² What will lower courts say about real-time CSLI collection?

On the one hand, it is clear that the majority opinion is quite worried about the time-travel nature of the CSLI database, which isn’t implicated in the same way by real-time data gathering.¹²³ Real-time CSLI gathering can be “switched on” for a specific target, allowing it to be pinpointed rather than amassed indiscriminately.

But on the other hand, retrospectivity is just one version of problematic “breadth,” and should be seen as such, rather than being treated as a necessary requirement. There might be databases that collect a broad swath of data across time without being retrospective in the same way as the CSLI database. One example would be a police order commanding a phone company to collect CSLI in real-time about one individual for seven days.¹²⁴ Or consider a database that stores

119. See, e.g., KERR, DIGITAL FOURTH AMENDMENT, *supra* note 115 (arguing that *Carpenter* should not turn on the amount of information obtained).

120. *Carpenter*, 138 S. Ct. at 2220 (declining to express an opinion about “real-time CSLI”).

121. *Id.*

122. *Id.* at 2218 (“With access to CSLI, the Government can now travel back in time to retrace a person’s whereabouts”); *id.* at 2234 (Kennedy, J., dissenting) (listing factors including retrospectivity); *id.* at 2223 (majority opinion) (listing factors not including retrospectivity).

123. *Id.* at 2218. The metaphor of treating police access to historical data as travel in a time machine was first proposed by legal scholar Steven Henderson. Henderson, *supra* note 63, at 935.

124. Compare *Jones v. United States*, 168 A.3d 703, 713 (D.C. 2017) (holding that use of a cell-site simulator to locate a suspect’s phone in real time “invaded a reasonable expectation of privacy and was thus a search”), with *United States v. Riley*, 858 F.3d 1012, 1018 (6th Cir. 2017), *cert. denied*, 138 S. Ct. 2705 (2018) (holding that “government did not conduct a search under the Fourth Amendment when it tracked the real-time GPS coordinates of” suspect’s phone outside the home for seven hours). Other courts avoided answering whether

retrospective information only about some people but not everybody in the database.¹²⁵ So long as the information is deep, broad, and of comprehensive reach, it should trigger this factor, whether or not it is retrospective in the same way.

3. Third Factor: The Inescapable and Automatic Nature of the Collection

The first two factors focus on the information's intrinsic nature. They analyze information as a database designer would, examining the qualitative and quantitative content of the data and the inferences that can be drawn from it. The third factor, in contrast, operates in a much more traditional mode, focusing on what the database owner and data subject have done (or could have done).

The third and final factor is the "inescapable and automatic nature" of how the information is collected.¹²⁶ This factor speaks to whether the targets of the surveillance may have assumed the risk of the data collection or knowingly exposed their information to the private party.¹²⁷ This factor (really two separate factors) brings into the analysis the idea that individuals might sometimes relinquish their Fourth Amendment rights when they assume the risk of surveillance, for example by publishing information to the general public.

Some forms of data collection are *inescapable* because they relate to services one needs to use to be a functioning member of today's society. In the case of CSLI, cell phones are "'such a pervasive and insistent part of daily life' that carrying one is indispensable to

obtaining real-time data constitutes a search. *See, e.g.,* United States v. Wallace, 866 F.3d 605, 609 (5th Cir. 2017), *withdrawn and superseded*, 885 F.3d 806 (5th Cir. 2018) (noting that it is an open question whether it is a search to obtain real-time E911 data but nonetheless holding that police were covered by good-faith exception to exclusionary rule); United States v. Banks, 884 F.3d 998, 1012–13 (10th Cir. 2018) (declining to decide whether "tracking a cell-phone's real-time location is a search" because parties did not thoroughly brief the issue, but, assuming that it was a search, finding exigent circumstances exception applied). *See generally* Eric Lode, Annotation, *Validity of Use of Cellular Telephone or Tower to Track Prospective, Real Time, or Historical Position of Possessor of Phone Under Fourth Amendment*, 92 A.L.R. Fed. 2d 1 (2015).

125. For example, under the USA FREEDOM Act of 2015, the NSA can request telephony metadata records relating to a suspect and everyone within "two hops" of contact with the suspect. 50 U.S.C. § 1861(c)(2)(F)(iii)–(iv) (2012 & Supp. III 2015) (permitting "the prompt production of a first set" and "a second set of call detail records"). Researchers estimate that this can net the records of approximately 25,000 subscribers with a single search. Jonathan Mayer et al., *Evaluating the Privacy Properties of Telephone Metadata*, 113 PROC. NAT'L ACAD. SCI. 5536, 5538 (2016).

126. *Carpenter*, 138 S. Ct. at 2223.

127. *Id.* at 2220 ("Apart from disconnecting the phone from the network, there is no way to avoid leaving behind a trail of location data. As a result, in no meaningful sense does the user voluntarily 'assume[] the risk' of turning over a comprehensive dossier of his physical movements.") (quoting *Smith v. Maryland*, 442 U.S. 735, 745 (1979)).

participation in modern society.”¹²⁸ The *Carpenter* opinion makes this point in dramatic fashion by borrowing from Chief Justice Roberts’s opinion in *Riley*:

Unlike the bugged container in *Knotts* or the car in *Jones*, a cell phone — almost a “feature of human anatomy,” *Riley*, 573 U.S., at —, 134 S. Ct., at 2484 — tracks nearly exactly the movements of its owner. While individuals regularly leave their vehicles, they compulsively carry cell phones with them all the time. A cell phone faithfully follows its owner beyond public thoroughfares and into private residences, doctor’s offices, political headquarters, and other potentially revealing locales. See *id.*, at —, 134 S. Ct., at 2490 (noting that “nearly three-quarters of smart phone users report being within five feet of their phones most of the time, with 12% admitting that they even use their phones in the shower”); contrast *Cardwell v. Lewis*, 417 U.S. 583, 590, 94 S. Ct. 2464, 41 L.Ed.2d 325 (1974) (plurality opinion) (“A car has little capacity for escaping public scrutiny.”).¹²⁹

Perhaps reflecting how some members of modern society feel shackled to these devices, Chief Justice Roberts deploys an especially evocative simile: “when the Government tracks the location of a cell phone it achieves near perfect surveillance, as if it had attached an ankle monitor to the phone’s user.”¹³⁰

Inescapability is not the same as the *automatic* nature of the information collected. CSLI is automatically part of cell service because the records are generated whenever the service is used and there is no meaningful opportunity to opt out.¹³¹

[A] cell phone logs a cell-site record by dint of its operation, without any affirmative act on the part of the user beyond powering up. Virtually any activity on the phone generates CSLI, including incoming calls, texts, or e-mails and countless other data connections that a phone automatically makes when checking for news, weather, or social media updates. Apart from disconnecting the phone from the network, there is no

128. *Carpenter*, 138 S. Ct. at 2220 (quoting *Riley v. California*, 134 S. Ct. 2473, 2484 (2014)).

129. *Id.* at 2218.

130. *Id.*

131. *Id.* at 2220.

way to avoid leaving behind a trail of location data. As a result, in no meaningful sense does the user voluntarily “assume[] the risk” of turning over a comprehensive dossier of his physical movements.¹³²

Once again, lower courts might have difficulty applying this factor to technologies that collect data automatically, but not inescapably — such as mobile apps that are voluntarily installed and can be deleted with one click — or those that do so inescapably, but not automatically — such as a doctor’s manual logging of a consenting patient’s symptoms.

4. The Test

To summarize, *Carpenter* promulgates a new three-factor test that should be applied not necessarily to the specific facts of a case but rather to the category of information being sought. In conducting the test, a court should ask whether a given category of information (1) has a deeply revealing nature; (2) possesses depth, breadth, and comprehensive reach; and (3) results from an inescapable and automatic form of data collection.

D. Applying the Carpenter Test

Under this test, what other databases full of third-party-collected records are likely to be found protected by a reasonable expectation of privacy and fall outside the third-party doctrine? Consider a few examples.

1. Very Likely Covered: Web Browsing Records

I am confident that the *Carpenter* test will extend Fourth Amendment protection to web-browsing records collected by ISPs (or browser or operating system manufacturers). Justice Kennedy raises this prospect, complaining that the majority opinion doesn’t reveal whether the seven-day threshold “should apply to information like IP addresses or website browsing history.”¹³³

Web browsing records possess a deeply revealing nature even if they record only the IP addresses of websites visited.¹³⁴ In 2009, I argued that “[t]he potential inconvenience, embarrassment, hardship, or

132. *Id.*

133. *Id.* at 2234 (Kennedy, J., dissenting).

134. See generally Ohm, *Invasive ISP Surveillance*, *supra* note 9, at 1444.

pain that could result from the trove of data of [ISP] monitoring is limited only by the wickedness of one's imagination."¹³⁵ More recently, I testified to Congress that:

The list of websites an individual visits, available to a [broadband Internet access service] provider even when https encryption is used, reveals so much more than a member of a prior generation would have revealed in a composite list of every book she had checked out, every newspaper and magazine she had subscribed to, every theater she had visited, every television channel she had clicked to, and every bulletin, leaflet, and handout she had read. No power in the technological history of our nation has been able until now to watch us read individual articles, calculate how long we linger on a given page, and reconstruct the entire intellectual history of what we read and watch on a minute-by-minute, individual-by-individual basis.¹³⁶

Similarly, Neil Richards has written about the sensitivity of records of "intellectual privacy" like these.¹³⁷ "Intellectual records — such as lists of Web sites visited, books owned, or terms entered into a search engine — are in a very real sense a partial transcript of the operation of a human mind. They implicate the freedom of thought and the freedom of intellectual exploration."¹³⁸ He argues that First Amendment concerns add a gloss to the Fourth Amendment and so access to records like these should require warrants.¹³⁹

The efficiency gain represented by web-browsing records is profound. Just as CSLI has given the police unprecedented power to track the location of targets at very low costs, web browsing records, for the first time in human history, have given the police access to the reading habits of millions of users with very little expense or effort.¹⁴⁰

The "depth, breadth, and comprehensive nature" factor is sure to be more contestable when applied to web browsing records. This precise question has recently been debated publicly in the Federal Communications Commission, which enacted a sweeping broadband privacy rule in the final days of the Obama administration, only to have

135. *Id.*

136. *FCC Overreach: Examining the Proposed Privacy Rules: Hearing Before the H. Subcomm. on Comm'n & Tech. of the H. Comm. on Energy & Commerce*, 114th Cong. 5 (2016) (statement of Paul Ohm, Professor, Georgetown University Law Center).

137. See generally Neil M. Richards, *Intellectual Privacy*, 87 TEX. L. REV. 387 (2008).

138. *Id.* at 436.

139. *Id.* at 440.

140. *Id.*

Congress roll back the rule in the early days of the Trump administration.¹⁴¹ In those proceedings, ISP lobbyists argued that their view into individual reading habits was far from comprehensive — in *Carpenter*'s terms, they lacked depth and breadth — because individuals surf the web via different ISPs.¹⁴² In the course of a single day, many people surf on their phone, their home broadband connection, and their work connection, using a different ISP for each one.¹⁴³ The police might plausibly argue that this distinguishes web browsing data from CSLI because people tend to carry their cell phone in their pockets or purses throughout the day. Your cell phone works like a passive tracking device, sending pings to the nearest cell tower whenever you are using your phone and sometimes even when you are not.¹⁴⁴

Finally, the police might argue that web browsing records generated by an ISP are not “inescapable and automatic” in the same way as CSLI, because web browsing is both intentional and visible behavior — a record is logged whenever you use your phone or computer's web browser to access the web.¹⁴⁵

Lower courts thus might struggle with the uncertainty inherent in the multi-factor test. ISP-generated web browsing records are much more deeply revealing and represent more of an efficiency gain than CSLI records.¹⁴⁶ Although ISPs are deep, broad, of comprehensive reach, inescapable, and automatic, they might not rise for these factors to the same levels as CSLI.

However, I predict courts will have little difficulty holding that massive databases that record the IP addresses visited by an individual meet the three-factor test, even though a few factors cut in the other direction. Police access to these records will constitute a search and thus, the third-party doctrine will not extend to cover them. Going forward, the police are well-advised to seek records like these only after first obtaining a warrant.

141. See Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, 81 Fed. Reg. 87, 274 (Dec. 2, 2016) (to be codified at 47 C.F.R. pt. 64) (rule as enacted); S.J. Res. 34, 115th Cong. (2017) (joint resolution reversing the rule).

142. Peter Swire et al., *Online Privacy and ISPs: ISP Access to Consumer Data is Limited and Often Less than Access by Others* 24–25 (Feb. 29, 2016) (unpublished paper) (on file with The Institute for Information Security & Privacy at Georgia Tech), http://www.iisp.gatech.edu/sites/default/files/images/online_privacy_and_isps.pdf [<https://perma.cc/EC45-YWSP>].

143. *Id.*

144. *Carpenter v. United States*, 138 S. Ct. 2206, 2211 (2018) (“Most modern devices, such as smartphones, tap into the wireless network several times a minute whenever their signal is on, even if the owner is not using one of the phone's features.”).

145. *Cf. Ohm, Invasive ISP Surveillance*, *supra* note 9, at 1476 (describing the automatic nature of ISP surveillance, but concluding that it is conducted without meaningful consent).

146. *Id.* at 1444; Richards, *supra* note 137, at 436.

2. Most Likely Covered: Massive Collections of Telephone and Bank Records

Perhaps counter-intuitively, the police most likely now need a warrant to obtain massive collections of phone records or bank records, the same category of records held not to require a warrant in the third-party doctrine cases *Smith v. Maryland*¹⁴⁷ and *Miller v. United States*.¹⁴⁸ Even though the Court declined to overturn *Smith* and *Miller*, hints throughout the *Carpenter* opinions suggest that, some day, these two opinions will be narrowed to the facts of those 1970s cases.¹⁴⁹

Bank records and phone records can be as deeply revealing as CSLI. *Carpenter's* dissenting opinions make this plain. Justice Kennedy concludes that “[t]he troves of intimate information the Government can and does obtain using financial records and telephone records dwarfs what can be gathered from cell-site records.”¹⁵⁰ Justice Gorsuch asks, “[w]hy is someone’s location when using a phone so much more sensitive than who he was talking to (*Smith*) or what financial transactions he engaged in (*Miller*)?”¹⁵¹ These passages will be quoted the first time a defendant challenges the warrantless access by the police to large quantities of this kind of information. Say the police use a subpoena to obtain years of credit card transactions or the NSA uses a sub-warrant process to obtain millions of telephone metadata. It is now quite likely that courts will require a warrant for this kind of information, citing *Carpenter's* new test.

These courts will now be able to distinguish *Smith* and *Miller* because modern technology tends to produce databases of telephone or financial information that are far more voluminous and detailed than the records at issue in those 1970s cases. With the ubiquity of credit and the decline of cash, almost every commercial transaction we make ends up in a bank record. These might today include great detail about what has been purchased, or a note by the merchant. Similarly, more communications metadata is being collected by today’s telephones than in the past. Computer storage is much cheaper and easier to access than the paper records of the 1970s, reducing the incentive to ever delete anything.¹⁵²

This shines new light on the dueling 2013 district court opinions that assessed the legality of the NSA’s massive telephony metadata pro-

147. 442 U.S. 735 (1979).

148. 425 U.S. 435 (1976).

149. *Carpenter*, 138 S. Ct. at 2217 (declining to extend but not overturning *Smith* and *Miller*).

150. *Id.* at 2232 (Kennedy, J., dissenting).

151. *Id.* at 2262 (Gorsuch, J., dissenting).

152. See generally VIKTOR MAYER-SCHÖNBERGER, DELETE: THE VIRTUE OF FORGETTING IN THE DIGITAL AGE 62–67 (2011).

gram, one distinguishing *Smith* and the other feeling bound by the precedent. The opinions assessed the legality of the program revealed to the public by Edward Snowden, through which the NSA gathered the non-content phone records, such as the originating and receiving telephone numbers of phone calls made by millions of Americans.¹⁵³ In *Klayman v. Obama*,¹⁵⁴ Judge Richard Leon of the District Court for the District of Columbia held that the telephony program likely violated the Fourth Amendment, expressly declining to follow *Smith*.¹⁵⁵ “[T]he *Smith* pen register and the ongoing NSA Bulk Telephony Metadata Program have so many significant distinctions between them that I cannot possibly navigate these uncharted Fourth Amendment waters using as my North Star a case that predates the rise of cell phones.”¹⁵⁶ Less than two weeks later, Judge William Pauley, in *ACLU v. Clapper*,¹⁵⁷ came to the opposite conclusion, finding that *Smith* controlled.¹⁵⁸ “Because *Smith* controls, the NSA’s bulk telephony metadata collection program does not violate the Fourth Amendment.”¹⁵⁹

History, in the form of *Carpenter*, has been much kinder to Judge Leon. A lower court judge trying to rule today that *Smith* controls would have to work much harder than Judge Pauley had to in distinguishing *Carpenter*. Judge Pauley’s reasoning seemed essentially to be that zero times a massive number is still zero. *Smith* found no protectable Fourth Amendment interest in the numbers dialed by a single telephone customer, and therefore, there must also be no Fourth Amendment interest for the collection of the dialing habits of tens of millions of customers.¹⁶⁰

Carpenter makes clear that the scale of data collection matters.¹⁶¹ Constitutionally meaningful privacy can spring forth when records amass in the millions. Judge Pauley’s reasoning should now be seen as defective, especially held next to Judge Leon’s approach, which anticipated the *Carpenter* reasoning, albeit using different factors and language. Judge Leon offered four reasons to distinguish the NSA program

153. Laura K. Donohue, *Bulk Metadata Collection: Statutory and Constitutional Considerations*, 37 HARV. J.L. & PUB. POL’Y 757, 760 (2014).

154. 957 F. Supp. 2d 1 (D.D.C. 2013), *vacated on other grounds*, 800 F.3d 559 (D.C. Cir. 2015).

155. *Id.* at 37.

156. *Id.*

157. 959 F. Supp. 2d 724 (S.D.N.Y. 2013), *vacated on other grounds*, 785 F.3d 787 (2d Cir. 2015).

158. *Id.* at 752.

159. *Id.*

160. *Id.* (“The fact that there are more calls placed does not undermine the Supreme Court’s finding that a person has no subjective expectation of privacy in telephony metadata.” (citing *Smith v. Maryland*, 442 U.S. 735, 745 (1979))).

161. *Carpenter v. United States*, 138 S. Ct. 2206, 2219 (2018) (“There is a world of difference between the limited types of personal information addressed in *Smith* and *Miller* and the exhaustive chronicle of location information casually collected by wireless carriers today.”).

from the facts of *Smith*. First, *Smith* involved data collected over a shorter time frame — 14 days versus months or years.¹⁶² Second, the detailed program between the NSA and the telephone companies created a far more intertwined relationship than the one-off request in *Smith*.¹⁶³ Third, the NSA had the technological capability “to store and analyze the phone metadata of every telephone user in the United States,” providing perhaps the closest parallel between this opinion and *Carpenter*.¹⁶⁴ Finally, telephony metadata can reveal much more sensitive information than the phone records of the late-1970s.¹⁶⁵

Had Judge Leon’s opinion been written after *Carpenter*, it would have been seen as a direct application of the new opinion. Massive databases of telephony records implicate every one of Chief Justice Roberts’s concerns about CSLI. The NSA’s program implicated the Fourth Amendment, notwithstanding the supposed continued vitality of *Smith*. Just like in *Carpenter* itself, I predict courts would “decline to extend *Smith* and *Miller*” to NSA-scale databases of telephony metadata.¹⁶⁶

3. Uncertain Application: Databases of Medical Records and Genetic Information

The examples covered so far — massive databases of web browsing habits, telephone dialing records, and financial records — each satisfy all, or nearly all, of the three *Carpenter* factors and thus, are likely to be found searches. But other databases of investigatory interest face a far less certain fate under the new test.

Under rules promulgated under the Health Insurance Portability and Accountability Act (“HIPAA”), law enforcement, with a grand jury subpoena, can access medical records stored by a covered provider.¹⁶⁷ Has *Carpenter* upset this rule, rendering this regulatory scheme now unconstitutional? Does a large database of health information now require a warrant to access?

For two of the three *Carpenter* factors, one could argue that medical records deserve as much or even more protection than CSLI. Medical records contain symptoms, diagnoses, and prescriptions — information likely far more deeply revealing than location information.¹⁶⁸ Even compared to owning a smartphone, individuals cannot easily choose to avoid professional medical care, making the production of these records more inescapable and automatic. The breadth and efficiency gain

162. *Klayman v. Obama*, 957 F. Supp. 2d 1, 32 (D.D.C. 2013).

163. *Id.* at 32–33.

164. *Id.* at 33.

165. *Id.* at 33–34.

166. *Carpenter*, 138 S. Ct. at 2220.

167. 45 C.F.R. § 164.512(f)(1)(ii) (2018) (permitting disclosure of protected health information pursuant to a court order or grand jury subpoena).

168. See Ohm, *Sensitive Information*, *supra* note 87, at 1150–53.

sub-factors probably weigh about the same for these records as for CSLI: most medical providers keep records dating back to the beginning of their interaction with a patient and it would cost the police an exorbitant sum to compile the kind of information it can access for very little.

The other subfactors and factors cut the other way. The main sub-factor that distinguishes CSLI from medical records is depth. The metronomic regularity with which an individual's location is tracked seemed quite important to the majority opinion.¹⁶⁹ In contrast, most people interact with the health care system only on occasion.¹⁷⁰

Finally, while the creation of medical records might be as inescapable as CSLI, they usually are not as automatic. Unlike the take-it-or-leave-it and invisible quality of CSLI gathering, most medical records are populated in clearly delineated interactions, when we are aware that we are literally being poked, prodded, and measured.

For these reasons, lower courts will likely consider medical record data to be a relatively close call. For ordinary healthy individuals, their medical records — while undoubtedly sensitive — are not nearly the product of the same kind of “tireless and absolute surveillance” at issue in *Carpenter*.¹⁷¹ The digitization of these records has not experienced the same dramatic gains in efficiency as the tracking of location or reading habits.

What about a copy of an individual's DNA stored with a private third party? In his dissent, Justice Gorsuch opines without analysis that “most lawyers and judges today” would require a warrant and probable cause to access DNA voluntarily stored with 23andMe.¹⁷² This provides an important window into Justice Gorsuch's baseline attitude about the Fourth Amendment and might also offer a window into how to directly appeal to him in the future. But this conclusion certainly doesn't flow from the *Carpenter* factors.

Without a doubt, a copy of an individual's genome satisfies the deeply revealing nature factor. Genetic information reveals propensity for disease, physical and mental characteristics, parentage, and genealogy.¹⁷³ It reveals this not only for the individual who uploaded the DNA but also for close relatives.¹⁷⁴

169. See *Carpenter*, 138 S. Ct. at 2218.

170. The exceptions are hospitalized patients and people diagnosed with chronic or terminal conditions. Many of these people might be connected to 24/7 electronic devices that generate information in exactly the same fashion as a smart phone.

171. *Id.*

172. *Id.* at 2262 (Gorsuch, J., dissenting).

173. Mike Silvestri, Note, *Naturally Shed DNA: The Fourth Amendment Implications in the Trail of Intimate Information We All Cannot Help But Leave Behind*, 41 U. BALT. L. REV. 165, 168 (2011).

174. Erin Murphy, *Relative Doubt: Familial Searches of DNA Databases*, 109 MICH. L. REV. 291, 313 (2010).

None of the other factors seem to trigger the same concerns as CSLI. A single copy of the three billion base pairs that comprise a human DNA does not track activity and change over time, unlike most of the other examples we have considered. At least under 23andMe's current business model, submissions are fundamentally voluntary, although individuals who did not submit their DNA will be able to argue about the inescapable nature of their presence in close relatives' genetic data if the police target them through their relatives' submissions.¹⁷⁵

It seems unlikely that a court would require a warrant for DNA evidence held by a private third party based on a straight application of the *Carpenter* factors. This is not to say that there might not be other applications of the REP test that would protect this information. It is a reminder that *Carpenter* is not the only path to finding that a Fourth Amendment search has occurred.

The basic rule of *Carpenter* alone presents a fundamental change to Fourth Amendment doctrine. It requires a warrant in many situations where none were required before. But this important change is just the first of many found within the reasoning of this opinion.

III. BEYOND THE CORE TEST OF *CARPENTER*

Based on the new substantive rule it announces, *Carpenter* is already on par with some of the most consequential Fourth Amendment cases of all time. But when you look beyond the core rule to some of the other revolutions wrought in the opinion, it is possible to conclude that *Carpenter* represents a fundamental shift, not merely an incremental adaptation. It turns the third-party doctrine inside out, requiring the government to account for the database design and information-gathering decisions of private parties, decisions made without any state intervention. Its broad reasoning will apply not only when third parties are involved but also when the government conducts detailed digital surveillance by itself. It also creates three new rules of technological equivalence, which are much more straightforward to apply than the multi-factor test and therefore, might end up being applied more often than the core rule itself.

A. *Carpenter* as a Replacement for *Katz*

The conventional wisdom suggests that *Carpenter* is an application or expansion of the *Katz* REP test. We might think of it instead as an outright replacement for REP, at least for cases involving complex modern technology.

175. *Id.* at 297–301, 337 (explaining the mechanics behind familial searches through DNA databases in criminal cases).

Carpenter settles long-standing disputes about both prongs of the *Katz* test. It affirms the conclusion that “*Katz* Has Only One Step”¹⁷⁶ by providing no analysis whatsoever into the defendant’s subjective expectation of privacy. For the objective prong, *Carpenter* means that the Court has at long last answered the fundamental question about REP: does the objective prong merely describe the expectations of ordinary Americans or does it ask judges to propound a normative vision for the kind of society the Constitution seeks to protect? *Carpenter* selects the normative over the descriptive: the role of courts is to protect the balance of power between the state (in the form of the police) and the people, refusing to let technological change eviscerate individual privacy and security from the state.¹⁷⁷

These changes do more than apply or extend *Katz*. They reinvent and supplant that venerable opinion. The REP test has been replaced by *Carpenter*’s multi-factor test and the rule of technological equivalence. Time will reveal that the *Katz* era has ended. This is a welcome development; the *Carpenter* era will be seen as more predictable, constitutionally supported, and responsive to the rate of technological change than the REP test it has replaced.

1. The Subjective Prong: *Katz* Has Only One Step

Carpenter supports what Orin Kerr has argued: “the subjective prong [of the REP test] has become a phantom doctrine.”¹⁷⁸ As initially expressed in Justice Harlan’s concurrence, the REP test was a two-pronged inquiry: “first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as ‘reasonable.’”¹⁷⁹

Scholars have offered at least three different interpretations for the subjective prong, none of which appear in *Carpenter*. Most often, courts seem to treat the subjective test as an inquiry into what the person actually intended in her mind.¹⁸⁰ Did this person actually believe her actions or communications were shielded from public view? The problem with this formulation is that it never seems to matter. Almost never is a court confronted with a situation in which this version of the subjective prong fails but the objective prong does not.¹⁸¹

176. See generally Orin S. Kerr, *Katz Has Only One Step: The Irrelevance of Subjective Expectations*, 82 U. CHI. L. REV. 113, 113 (2015) [hereinafter Kerr, *One Step*].

177. *Carpenter*, 138 S. Ct. at 2246.

178. Kerr, *One Step*, *supra* note 176, at 133.

179. *Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

180. Kerr, *One Step*, *supra* note 176, at 130–31.

181. See *id.* at 116–22 (examining all published opinions analyzing the Fourth Amendment reasonable expectation of privacy test in 2012 and finding that not a single case “relied on the subjective test in an outcome-determinative way”).

Kerr argues that the subjective prong could instead have been read, long ago, to place more emphasis on Justice Harlan's use of the word "exhibited."¹⁸² By this reading, the subjective prong asks whether the defendant had "voluntarily exposed" information to the public. Critically, this version of the test would not require courts to probe the inner mind of the person asserting privacy. Rather, it would look to the objective measures the person took to block the government's view.¹⁸³

A third way of interpreting the subjective prong is offered by Lior Strahilevitz and Matthew Kugler.¹⁸⁴ They argue that courts should consult survey evidence in the subjective prong, "us[ing] the sentiments of the median American citizen as a proxy for the defendant's subjective expectation of privacy."¹⁸⁵

We do not know how the *Carpenter* court interpreted the subjective prong because the majority's opinion gives it almost no attention. The opinion never mentions the word "subjective." Its recitation of the REP test barely nods at this as a separate requirement: An REP is "[w]hen an individual 'seeks to preserve something as private,' and his expectation of privacy is 'one that society is prepared to recognize as reasonable'"¹⁸⁶ In applying the test, the Court makes no attempt to analyze subjective and objective expectations separately.

Carpenter did not put a nail in the coffin of the subjective prong, because it was interred long ago.¹⁸⁷ The subjective prong has become an unmarked grave, one courts trample from above, not even acknowledging the presence of the decomposed remains underfoot.

2. The Objective Prong: Victory of the Normative Fourth Amendment

By recognizing tech exceptionalism, the *Carpenter* court restores — at least for the time being — the normative vision of the Fourth Amendment, taking sides in a very old debate: is the objective prong of the REP test — which asks, is society prepared to accept an expectation of privacy as reasonable — a descriptive or normative inquiry?¹⁸⁸ Is it the judge's role to examine what the reasonable individual or median member of society expects, or is it the judge's charge to

182. *Id.* at 127.

183. *Id.* at 126.

184. Matthew B. Kugler & Lior Jacob Strahilevitz, *Actual Expectations of Privacy, Fourth Amendment Doctrine, and the Mosaic Theory*, 2015 SUP. CT. REV. 205, 240–44 (2015) [hereinafter Kugler & Strahilevitz, *Actual Expectations*].

185. *Id.* at 241.

186. *Carpenter v. United States*, 138 S. Ct. 2206, 2213 (2018).

187. Kerr, *One Step*, *supra* note 176, at 114 (attributing abandonment of subjective prong to cases from the 1970s and 1980s).

188. Anthony G. Amsterdam, *Perspectives on the Fourth Amendment*, 58 MINN. L. REV. 349, 382–84, 391–93, 404 (1974).

imagine how the court's rulings can help set our society onto a particular path?¹⁸⁹

Justice Harlan, who first conceived of the REP test, made his opinion about this question quite clear only four years after *Katz*, albeit in dissent:

Since it is the task of the law to form and project, as well as mirror and reflect, we should not, as judges, merely recite the expectations and risks without examining the desirability of saddling them upon society. The critical question, therefore, is whether under our system of government, as reflected in the Constitution, we should impose on our citizens the risks of the electronic listener or observer without at least the protection of a warrant requirement.¹⁹⁰

Too often, the Court has strayed from this path, thinking of its role in interpreting REP as merely descriptive.¹⁹¹

Carpenter advances the idea that, at least when police surveillance technology changes rapidly, the proper role for the court is the normative one Justice Harlan advocated. We should not saddle society with merely what it has come to expect.¹⁹²

Tech exceptionalism once again settles this question. The proper accounting of the way technology has disrupted individual privacy, distorted society, and rebalanced the power between the state and its citizens thrusts the judiciary into a more aggressive role in interpreting the Fourth Amendment than it has assumed in the past.

This, once again, is at the heart of Orin Kerr's equilibrium adjustment theory and Bankston and Soltani's theory of government efficiency gain.¹⁹³ The Constitution is premised on an ordinary rate of change in the balance of power between the state and the people. The Fourth Amendment is our national thermostat, recalibrating what the

189. Kerr, *Four Models*, *supra* note 89, at 507–24.

190. *United States v. White*, 401 U.S. 745, 786 (1971) (Harlan, J., dissenting).

191. *See, e.g., Bond v. United States*, 529 U.S. 334, 338 (2000) (“When a bus passenger places a bag in an overhead bin, he expects that other passengers or bus employees may move it for one reason or another. Thus, a bus passenger clearly expects that his bag may be handled.”); *California v. Ciraolo*, 476 U.S. 207, 215 (1986) (“In an age where private and commercial flight in the public airways is routine, it is unreasonable for respondent to expect that his marijuana plants were constitutionally protected from being observed with the naked eye from an altitude of 1,000 feet.”); *Smith v. Maryland*, 442 U.S. 735, 744 (1979) (“When he used his phone, petitioner voluntarily conveyed numerical information to the telephone company and ‘exposed’ that information to its equipment in the ordinary course of business. In so doing, petitioner assumed the risk that the company would reveal to police the numbers he dialed.”).

192. *Cf. Kerr, Four Models*, *supra* note 89, at 543–44.

193. Bankston and Soltani, *supra* note 70, at 335–38; Kerr, *Equilibrium-Adjustment*, *supra* note 73, at 84.

police can and cannot do. In periods of ordinary change for policing technology — which I believe describes the first two hundred years or so of our national experience — we could afford a merely descriptive Fourth Amendment, assigning to the courts a relatively passive role in mediating the relationship between state power and the people. But when faced with the disruptive technological restructuring of power and institutions, the normative Fourth Amendment — and the court's central role in protecting and strengthening it — becomes an imperative.

3. The Argument for Moving Beyond *Katz*

Once we recognize that *Carpenter* has moved beyond *Katz* in important ways, we should ask whether this is a desirable result. I contend that the future sketched out by *Carpenter* is preferable to the world *Katz* has given us.

First, *Carpenter*'s multi-factor test will lead to more predictability than *Katz*'s. The REP test has always been open-textured and ambiguous. What is a reasonable expectation of privacy? Is the objective prong to be analyzed descriptively or normatively?

Ambiguous at birth, the subsequent decades have done very little to lend *Katz* concreteness or predictability. Orin Kerr persuasively argues that the Court chooses from a menu of four different approaches — private facts, probabilistic, positive law, and policy — to assess REP.¹⁹⁴ But it is hard to discern a pattern to when the Court chooses each.¹⁹⁵

In contrast, the multi-factor test is relatively easy to apply. There will likely be disagreement about how to apply, say, the “depth, breadth, and comprehensive reach” factor to different databases.¹⁹⁶ But the spectrum of disagreement will be narrow and cabined compared to the wide ranging across Kerr's four models that *Katz* has created.¹⁹⁷ *Carpenter* sweeps away the cacophony of the four models, selecting a normative-over-descriptive methodology with three concrete factors.

Second, the approach is, if anything, more closely connected to the text and history of the Constitution. To be clear, neither *Katz* nor *Carpenter* purports to adhere closely to the text and history. But *Katz* suffered by focusing on a principle — privacy — that is nowhere to be seen in the literal text of the amendment.

194. Kerr, *Four Models*, *supra* note 89, at 506.

195. *Id.* at 524 (“The hard cases tend to be those in which the different models point judges to different conclusions. In those cases, courts must choose which model applies to that particular case.”).

196. See *supra* Section II.C.2 (discussing difficulty of the line-drawing inherent in these factors).

197. *Id.*

In contrast, *Carpenter*'s test and reasoning resonate much more directly with history. The Court primarily treats the Fourth Amendment as a restriction on government power, not just a protection of privacy.¹⁹⁸ The factors hone in on the features of data that fuel the government's power. "Comprehensive reach" allows the government to conduct surveillance on the entire populace; "breadth" allows it to peer back in time; "depth" and "deeply revealing nature" raise the prospect of meaningful harm.¹⁹⁹

In addition, the location information in *Carpenter* and the smart phone in *Riley* are arguably intrinsic aspects of individual personality, connecting them to the "persons" recited in the text of the Fourth Amendment.²⁰⁰

Third, the tech exceptionalism at the heart of the new test impels courts to engage in a deep consideration of the specific features of technology and society's embrace of technology that was usually lacking from the conventional REP test. This will prevent the kind of inadequate responsiveness to progress that plagued the third-party doctrine from its birth.

B. The Third-Party Doctrine, Inside Out

Carpenter concludes that location information is protected "[w]hether the Government employs its own surveillance technology as in *Jones* or leverages the technology of a wireless carrier"²⁰¹ This quote is breathtaking. It calls into question the bedrock rule that the Fourth Amendment concerns itself only with the activities of the government.²⁰² The police have never before had to account so fully for the independent decisions or actions of private actors. A private citizen could literally break into a house, break into a safe inside the house, steal what lay within the safe, and deliver the contents of the safe to the police.²⁰³ So long as the police had nothing to do with the thief before

198. *Carpenter v. United States*, 138 S. Ct. 2206, 2214 (2018) ("[T]he Amendment seeks to secure 'the privacies of life' against 'arbitrary power' [A] central aim of the Framers was 'to place obstacles in the way of a too permeating police surveillance.'").

199. *Supra* Section II.C.2.

200. U.S. CONST. amend. IV.

201. *Carpenter*, 138 S. Ct. at 2217.

202. *United States v. Jacobsen*, 466 U.S. 109, 113 (1984) ("This Court has also consistently construed this protection as proscribing only governmental action; it is wholly inapplicable to a search or seizure, even an unreasonable one, effected by a private individual not acting as an agent of the Government or with the participation or knowledge of any governmental official.").

203. *See United States v. Jarrett*, 338 F.3d 339, 347–48 (2006) (holding that receiving evidence from an anonymous hacker who had taken files from defendant's computer did not constitute government action and thus did not violate the Fourth Amendment).

he arrived at the stationhouse, they would be free to use the contents in court.²⁰⁴

For the first time, even though the police are not responsible for the decisions that led to the collection of potential evidence, they nevertheless are held to account for the nature of the information collected. This has blurred the government action requirement in some important ways.

Of the three *Carpenter* factors, the one that is most influenced by the choices made by private actors is “depth, breadth, and comprehensive reach.”²⁰⁵ To be clear, the Court does not seem to be delving into the motivations of cell phone providers; warrant suppression hearings will not turn on the testimony of a T-Mobile executive explaining why the company structures its data the way it does. But the constitutional meaning of the word “search” in cases like these now turns intrinsically on the results of the business decisions of companies.

Consider the breadth factor. The majority opinion emphasizes the importance of the “time machine” quality of CSLI. “With access to CSLI, the Government can now travel back in time to retrace a person’s whereabouts, subject only to the retention policies of the wireless carriers, which currently maintains records for up to five years.”²⁰⁶ For the most part, at least in the United States, corporate retention policies are not set by regulation.²⁰⁷ Each company must weigh the potential benefits of having access to old data against the cost of data storage and the potential trouble in the form of cybersecurity risk or regulatory scrutiny. Practices vary widely even between companies in the same industry.²⁰⁸ These choices are not made in consultation with the police, yet *Carpenter* has now given these private decisions constitutional weight.²⁰⁹

204. *See id.*

205. *Carpenter*, 138 S. Ct. at 2223.

206. *Id.* at 2218.

207. *See* Catherine Crump, Note, *Data Retention: Privacy, Anonymity, and Accountability Online*, 56 STAN. L. REV. 191, 193 (2003) (discussing the role of “data preservation” in the United States, in the absence of a data retention mandate). One rare exception is that the FCC requires telephone companies to keep billing information about telephone toll calls for eighteen months. 47 C.F.R. § 42.6 (2019). In 2006, the European Union enacted a Data Retention Directive that mandated providers of some communications services to retain certain data for six to twenty-four months. Council Directive 2006/24, art. 1, 2006 O.J. (L 105) 54 (EC). It was declared invalid by the Court of Justice of the European Union in 2014. Joined Cases C-293/12 & C-594/12, *Digital Rights Ir. Ltd. v. Ireland* (Apr. 8, 2014), <http://curia.europa.eu/juris/document/document.jsf?text=&docid=162437&pageIndex=0&doclang=en&mode=req&dir=&occ=first&part=1&cid=1539063> [https://perma.cc/PPQ9-LD6C].

208. Ernesto Van der Sar, *How Long Does Your ISP Store IP-Address Logs?*, TORRENT-FREAK (June 29, 2012), <https://torrentfreak.com/how-long-does-your-isp-store-ip-address-logs-120629> [https://perma.cc/SNR4-QEV4] (reporting IP address retention policies by ISPs from two weeks to eighteen months).

209. *Carpenter*, 138 S. Ct. at 2218 (focusing on importance of fact that CSLI is stored for five years).

The same can be said for the depth factor. Every company decides how much information to track and retain. Returning again to web-browsing surveillance, some ISPs retain very little evidence of the web browsing habits of their customers; others deploy deep packet inspection to view and store information about the content of communications between individuals and websites.²¹⁰ The first time the government is forced to defend against a challenge to the warrantless access to this kind of information, its fate might turn on where the ISP chose to position itself along this spectrum.

It could be argued, then, that the Court did more than narrow the third-party doctrine; it turned the third-party doctrine inside out. Not only does the mere fact that a target trusted personal information with a third party no longer insulate that data from Fourth Amendment scrutiny, the constitutional duties imposed on the police might also now turn on the independent decisions of third parties.

C. Carpenter and Direct Government Surveillance

Carpenter's reasoning should apply even when third parties are not involved. Its multi-factor test focuses most of its attention on the quality of the database alone, so it should apply even to databases compiled directly by the government. It might apply, for example, to analyze the use by the police of suspicionless, automated data collection techniques such as drone monitoring or facial recognition techniques used on surveillance camera data.²¹¹

Consider automated license plate readers ("ALPRs").²¹² These devices contain stationary cameras that sit for days, weeks, or longer on the side of the road, deployed by government officials for the express purpose of recording the license plate numbers of cars that pass by a particular location.²¹³ These records are fed into databases from which the police can search for particular vehicles and that are sometimes automatically searched to locate stolen or unregistered cars, kidnap victims, or missing persons.²¹⁴

A simplistic view of *Carpenter* would assume it had nothing to say about ALPRs. Because this technology does not involve private parties

210. Ohm, *Invasive ISP Surveillance*, *supra* note 9, at 1432–37.

211. GARVIE ET AL., *supra* note 60, at 31–33.

212. Rachel Levinson-Waldman, *Hiding in Plain Sight: A Fourth Amendment Framework for Analyzing Government Surveillance in Public*, 66 EMORY L.J. 527, 544–46 (2017). See generally Randy L. Dryer & S. Shane Stroud, *Automatic License Plate Readers: An Effective Law Enforcement Tool or Big Brother's Latest Instrument of Mass Surveillance? Some Suggestions for Legislative Action*, 55 JURIMETRICS J. 225 (2015); Jessica Gutierrez Alm, Note, *The Privacies of Life: Automatic License Plate Recognition is Unconstitutional Under the Mosaic Theory of Fourth Amendment Privacy Law*, 38 HAMLINE L. REV. 127 (2015).

213. Dryer & Stroud, *supra* note 212, at 229–32.

214. Kimberly J. Winbush, *Use of License Plate Readers*, 32 A.L.R. 7TH ART. 8 (2017).

doing the data collection, this falls out of the potential application of the third-party doctrine.²¹⁵ Ignoring *Carpenter*, this case might be seen as a fairly straightforward application of Fourth Amendment cases involving plain view, knowing exposure, and reduced expectations of privacy in automobiles.²¹⁶ This simplistic view would suggest that no justification or judicial review is required to collect information with an ALPR — much less a search warrant.²¹⁷

The better reading is to understand that *Carpenter* has rewritten the rules for assessing the reasonable expectation of privacy in massive data gathering efforts, whether or not they are instigated by private actors.

How, then, does ALPR fare under the *Carpenter* factors? Because ALPR gives the police the ability to track the location and movement of cars, it seems superficially similar to CSLI. But because ALPR measures location only at fixed points throughout a city, it is likely to be seen as less problematic than CSLI for many of the *Carpenter* factors.²¹⁸ ALPR generates data that is neither as deep, broad, nor comprehensive as CSLI.²¹⁹ Because there is less data, it collectively is less deeply revealing than CSLI.²²⁰ For those who drive, ALPR is as inescapable and automatic as CSLI, but the same is not true for those with smartphones but not cars.

In the end, courts must balance these factors and determine whether ALPR implicates privacy enough to qualify as an invasion of a reasonable expectation of privacy. It is likely to be a very close call. But nothing in *Carpenter*'s reasoning or multi-factor test suggests that they apply only when third parties are involved.

215. To be clear, some ALPR implementations are run by private companies, who sell the data collected to state entities. See Justin Rolich, *In Just Two Years, 9,000 of these Cameras Were Installed to Spy on Your Car*, QUARTZ (Feb. 5, 2019), <https://qz.com/1540488/in-just-two-years-9000-of-these-cameras-were-installed-to-spy-on-your-car> [https://perma.cc/6VC4-5H2G] (describing spread of ALPR technology to private companies and the general public).

216. *New York v. Class*, 475 U.S. 106, 114 (1986) (holding no reasonable expectation of privacy in automobile's vehicle identification number); *Cardwell v. Lewis*, 417 U.S. 583, 590 (1974) (plurality opinion) ("One has a lesser expectation of privacy in a motor vehicle . . .").

217. *United States v. Yang*, No. 2:16-cr-231-RFB, 2018 WL 576827 at *6 (D. Nev. Jan. 25, 2018) (holding no reasonable expectation of privacy in data collected in commercial license plate location database).

218. Alm, *supra* note 212, at 151–52 (conceding that ALPR data is more intermittent and thus less sensitive than GPS data collected over the same period of time).

219. *Id.* See *Yang*, 2018 WL 576827, at *6 (distinguishing *Jones* because ALPR does not "provide[] continuous contemporaneous information about the location of a vehicle" and does not "create[] a travel history of all of the movements of the targeted vehicle").

220. Alm, *supra* note 212, at 151–52.

D. The New Rule of Technological Equivalence

Up to this point, I have focused almost entirely on the rules deriving from the majority opinion signed by five justices. Even more can be surmised by what the dissents added, because even though they disagreed with the majority's holding and reasoning, they provide tantalizing concessions suggesting that they too are willing to read the Fourth Amendment to cover more police conduct than the Court has recognized in the past. One must be careful not to read too much into dissents, naturally. I am placing stock in arguments made by Justices Gorsuch and Kennedy, who might have been making rhetorical points rather than hinting at their future votes.²²¹

With those caveats in mind, reading all of the Carpenter opinions together suggests a broad new rule of technological equivalence. Any police activity that is the modern-day equivalent of activity that has been long protected under the Fourth Amendment is now protected.²²²

The new test relies on a simple syllogism: the Court in the past has held that information in a particular, traditional privacy context is protected by the Fourth Amendment. A technology produces information that is a modern-day equivalent of the information produced in that traditional context. The information in the modern context is also protected by the Fourth Amendment.

There are three major strands of this new test in these opinions: activity that is technologically equivalent to prying into (1) the intimacy of the home, (2) into papers held in bailment, and (3) into private communications. Consider each in turn.

1. Information from Inside the Home

The rule of technological equivalence springs from *Kyllo*, the 2001 case involving police use of a thermal imaging device pointed at a suburban home in Florence, Oregon.²²³ To prove that the defendant was growing marijuana inside his home, they used the device to reveal the heat that emanated from powerful grow lights and compared it to the ordinary heat patterns of his neighbors.²²⁴ The Supreme Court, in an opinion by Justice Scalia, held that using a thermal imager on a home constituted a Fourth Amendment search.²²⁵

221. Justice Kennedy, of course, will not cast any future votes!

222. *Carpenter v. United States*, 138 S. Ct. 2206, 2230 (2018) (Kennedy, J., dissenting).

223. *Kyllo v. United States*, 533 U.S. 27, 29 (2001).

224. *Id.* at 29–30.

225. *Id.* at 34–35.

Carpenter cites two crucial propositions from *Kyllo*.²²⁶ The first is the idea that an inference can be a search.²²⁷ The second is the proposition that when courts assess the impact of rapidly changing technology under the Fourth Amendment, they look not only at the technology used in the facts of the case, but they also extrapolate to future, more powerful versions of the technology. “While the technology used in the present case was relatively crude, the rule we adopt must take account of more sophisticated systems that are already in use or in development.”²²⁸

Putting these together, the first rule of technological equivalence applies to any information that reveals details from inside the home. The centerpiece of Justice Scalia’s reasoning in *Kyllo* was that “in the home . . . all details are intimate details.”²²⁹ This kind of reasoning is quite likely to extend Fourth Amendment protection to the information generated by many devices that comprise the Internet of Things, because so much of it focuses on the interior of the home.²³⁰ Smart speakers such as the Amazon Echo and Google Home record sounds from the inside of a home.²³¹ Smart TVs record the entertainment consumed in a home.²³² The Nest thermostat records the temperature of the home.²³³ And the Ring doorbell records visitors to the home.²³⁴ The police can obtain records like these as evidence in criminal investigations.²³⁵

226. *Carpenter*, 138 S. Ct. at 2218–19.

227. *Kyllo*, 533 U.S. at 36; *id.* at 44 (Stevens, J., dissenting) (criticizing the majority: “For the first time in its history, the Court assumes that an inference can amount to a Fourth Amendment violation”).

228. *Id.* at 36.

229. *Id.* at 37.

230. See Andrew Guthrie Ferguson, *The Internet of Things and the Fourth Amendment of Effects*, 104 CALIF. L. REV. 805, 836–42 (2016).

231. Michael Harrigan, *Privacy Versus Justice: Amazon’s First Amendment Battle in the Cloud*, 45 W. ST. L. REV. 91, 91–93 (2017) (discussing government’s attempt to obtain Amazon Echo recording for a murder trial); Arielle M. Rediger, *Always-Listening Technologies: Who Is Listening and What Can Be Done About It*, 29 LOY. CONSUMER L. REV. 229, 231, 239–40 (2017) (discussing privacy implications of Amazon Echo and Google Home).

232. Whitson Gordon, *How to Stop Your Smart TV from Tracking What You Watch*, N.Y. TIMES (July 23, 2018), <https://www.nytimes.com/2018/07/23/smarter-living/how-to-stop-your-smart-tv-from-tracking-what-you-watch.html> [<https://perma.cc/78UB-4G27>].

233. Jillisa Bronfman, *Weathering the Nest: Privacy Implications of Home Monitoring for the Aging American Population*, 14 DUKE L. & TECH. REV. 192, 196–99 (2016) (discussing privacy implications of Nest Labs products); David C. Vladeck, *Consumer Protection in an Era of Big Data Analytics*, 42 OHIO N.U. L. REV. 493, 511 (2016) (discussing privacy implications of Google Nest and competitors).

234. Reed Albergotti, *How Amazon’s Latest Security Device Let People Spy on You*, THE INFORMATION (May 11, 2018, 7:01 AM), <https://www.theinformation.com/articles/how-amazons-latest-security-device-let-people-spy-on-you> [<https://perma.cc/E3RF-RC8N>] (discussing privacy vulnerability of Ring doorbell system).

235. James O’Toole, *Cops can access your connected home data*, CNN (June 16, 2014, 2:25 PM), <https://money.cnn.com/2014/06/16/technology/smart-home-footage/index.html> [<https://perma.cc/TJ3G-9KPS>] (discussing tech companies’ requirements to release home security footage to law enforcement).

The *rule of equivalence to the home* suggests that the police now need a warrant to obtain any of this information.²³⁶ The *Kyllo* reasoning suggests that we need not even consider the sensitivity or intimacy of the information obtained, because “all details are intimate details.”²³⁷

Notice that the technological equivalence rule is far simpler and more predictable to apply than the majority’s multi-factor test. Once the equivalence is made, the conduct is ruled a search, and the analysis ends. One need not endure the multi-factor gymnastics required to analyze the status of CSLI.

Just a few months after *Carpenter* was decided, the Seventh Circuit applied this rule. In *Naperville Smart Meter Awareness v. Naperville*,²³⁸ the court held that a city’s mandatory use of smart meters on homes constituted a search under the Fourth Amendment.²³⁹ Because different appliances produce different “load signatures,” “researchers can predict the appliances that are present in a home and when those appliances are used.”²⁴⁰ This “reveals when people are home, when people are away, when people sleep and eat, what types of appliances are in the home, and when those appliances are used.”²⁴¹ Although the case cites *Carpenter* in a brief passage declining to apply the third-party doctrine, its core reasoning is an application of *Kyllo*.²⁴²

2. Bailment

Both Justices Kennedy and Gorsuch lean on the law of bailment, suggesting a revitalization of this ancient legal concept by prosecutors and criminal defense lawyers. Consider Justice Gorsuch’s academic disquisition on the idea:

[T]he fact that a third party has access to or possession of your papers and effects does not necessarily eliminate your interest in them. Ever hand a private document to a friend to be returned? Toss your keys to a valet at a restaurant? Ask your neighbor to look after your dog while you travel? You would not expect the

236. See, e.g., Zack Whittaker, *Judge Orders Amazon to Turn Over Echo Recordings in Double Murder Case*, TECHCRUNCH (Nov. 14, 2018), <https://techcrunch.com/2018/11/14/amazon-echo-recordings-judge-murder-case> [<https://perma.cc/E6A2-SVNL>] (reporting a New Hampshire court’s grant of a police search warrant to access Amazon Echo recordings in a double murder case).

237. *Kyllo v. United States*, 533 U.S. 27, 37 (2001).

238. 900 F.3d 521 (7th Cir. 2018).

239. The court ruled that the search was reasonable because the smart meter information was gathered for a non-criminal-investigation government purpose, and the benefits of the program outweighed the intrusion on privacy. *Id.* at 527–29.

240. *Id.* at 524.

241. *Id.* at 526.

242. *Id.*

friend to share the document with others; the valet to lend your car to his buddy; or the neighbor to put Fido up for adoption. Entrusting your stuff to others is a *bailment*. A bailment is the “delivery of personal property by one person (the *bailor*) to another (the *bailee*) who holds the property for a certain purpose.” Black’s Law Dictionary 169 (10th ed. 2014) A bailee normally owes a legal duty to keep the item safe, according to the terms of the parties’ contract if they have one, and according to the “implication[s] from their conduct” if they don’t. 8 C. J. S., Bailments § 36, pp. 468-469 (2017). A bailee who uses the item in a different way than he’s supposed to, or against the bailor’s instructions, is liable for conversion. *Id.*, § 43, at 481 These ancient principles may help us address modern data cases too. Just because you entrust your data—in some cases, your modern-day papers and effects—to a third party may not mean you lose any *Fourth Amendment* interest in its contents. Whatever may be left of *Smith* and *Miller*, few doubt that e-mail should be treated much like the traditional mail it has largely supplanted—as a bailment in which the owner retains a vital and protected legal interest.²⁴³

Justice Kennedy, while not engaging with the idea at such length, seems to agree that modern-day equivalents to bailment ought not to be subject to the third-party doctrine.²⁴⁴

This reasoning, by two justices in dissent,²⁴⁵ signals quite clearly that the Court will someday rule that “modern-day papers and effects” held by third parties will be protected by the Fourth Amendment. This seems to describe almost perfectly the contemporary state of cloud computing. Services like Google Drive and Dropbox allow individuals to move their modern-day papers into the cloud.²⁴⁶ Services like Amazon Web Services create dedicated virtualized computers on cloud

243. *Carpenter v. United States*, 138 S. Ct. 2206, 2268–69 (2018) (Gorsuch, J., dissenting).

244. *Id.* at 2228 (Kennedy, J., dissenting) (noting that the private parties in *Smith* and *Miller* “were not bailees or custodians of the records” at issue); see also *id.* at 2259 n.6 (Alito, J., dissenting) (“[T]his is not a case in which someone has entrusted papers that he or she owns to the safekeeping of another, and it does not involve a bailment.”).

245. Four, if you include Justices Alito and Thomas, who signed Justice Kennedy’s dissent.

246. Mickey Meece, *A User’s Guide to Finding Storage Space in the Cloud*, N.Y. TIMES, (May 16, 2012), <https://www.nytimes.com/2012/05/17/technology/personaltech/a-computer-users-guide-to-cloud-storage.html> (last visited May 11, 2019); *What is Dropbox*, DROPBOX, <https://www.dropbox.com/features> [<https://perma.cc/23WP-MAFW>]; *Google Drive*, GOOGLE, <https://gsuite.google.com/products/drive/> [<https://perma.cc/FU2V-ZRXC>].

servers, which customers can fill with data, which other users are not permitted to access.²⁴⁷ If law enforcement tries to obtain any information stored on services such as these, it seems quite likely that lower courts will rule such accesses to be controlled by the *technological equivalence of bailment* rule, thus requiring a warrant.

3. Private Communications

Similarly, all nine justices signed onto opinions that declare that the police need a warrant to read the content of email messages.²⁴⁸ Although this is still dicta, it is stated clearly enough so that lower courts can and should begin to rely on the clear signal.

This is important because, to date, only one appellate court, the Sixth Circuit, has required the police to obtain a warrant to access the content of stored email messages, in the 2010 case *United States v. Warshak*.²⁴⁹ *Warshak* itself is cited approvingly in *Carpenter* in three separate opinions: the majority,²⁵⁰ and the dissents by Justices Kennedy,²⁵¹ and Gorsuch.²⁵²

This is yet another application of the rule of technological equivalence: the *rule of equivalence to private communications*. In the 1877 case of *Ex Parte Jackson*, the Court required a warrant to open sealed letters in the possession of the postal service.²⁵³ Emails, “the technological scion of tangible mail,” according to the *Warshak* court,²⁵⁴ are the modern equivalents of postal letters from the time of *Ex Parte Jackson*.

As noted above, all nine justices have now signaled they would hold that the contents of email are protected by the Fourth Amendment. The police must obtain a search warrant, or proceed under an exception to the warrant requirement such as exigent circumstances, to access the contents of email messages.²⁵⁵

It is likely that this rule will protect other forms of electronic communications other than email. Any person-to-person communications

247. Alex Hern, *Amazon Web Services: The secret to the online retailer's future success*, THE GUARDIAN, (Feb. 2, 2017, 2:00 AM), <https://www.theguardian.com/technology/2017/feb/02/amazon-web-services-the-secret-to-the-online-retailers-future-success> [https://perma.cc/4Y33-AVFR]; *What is AWS?*, AMAZON WEB SERVS., <https://aws.amazon.com/what-is-aws> [https://perma.cc/KYN9-Y5QR].

248. *Carpenter*, 138 S. Ct. at 2222; *id.* at 2230 (Kennedy, J., dissenting); *id.* at 2269 (Gorsuch, J., dissenting).

249. 631 F.3d 266, 288 (6th Cir. 2010).

250. *Carpenter*, 138 S. Ct. at 2222.

251. *Id.* at 2230.

252. *Id.* at 2269.

253. 96 U.S. 727, 733 (1877) (requiring a warrant to open sealed letters in the possession of the postal service).

254. 631 F.3d at 286.

255. *Id.* at 288.

are likely protected. The police most likely now need a warrant to obtain, from storage or in real-time, instant messages, direct messages on a social networking service, or text messages.²⁵⁶

Carpenter upends Fourth Amendment doctrine. Its most revolutionary contribution, however, might be what it has done to Fourth Amendment reasoning.

IV. CARPENTER'S TECH EXCEPTIONALISM

The beating heart of the *Carpenter* majority opinion is its deep and abiding belief in the exceptional nature of the modern technological era. This seems to come directly from Chief Justice Roberts, who revealed the same attitude four years earlier in the majority opinion in *Riley v. California*.²⁵⁷ Recent advances in technology such as the smartphone and the Internet have led to differences in kind and not merely in degree from the technology of the past.

The Chief Justice's break with the technological past supports a break with judicial precedent in several ways. A belief in the exceptionalism of modern technology leads one to dismiss otherwise conventional analogies. *Riley* and *Carpenter* both refuse to compare smartphones to past technologies, such as address books, diaries, or even telephones.²⁵⁸ Because analogical reasoning sits at the heart of legal reasoning and stare decisis, the Court's rejection of analogies like these gives it an opening to chart a new path.

Reasoning about exceptional technology requires courts to develop a deep understanding of technology, and these opinions are notable for the way they rely heavily on technological explication. They are full of citations to amici briefs and they press the boundaries of judicial notice.

Finally, the Court's adoption of tech exceptionalism closes the door on scholars who have been trying to reinvent *Katz* by appealing to surveys, history, or positive law. Each of these three approaches peers into our past and relies on the ability of lay people to understand what has changed. *Carpenter* and *Riley* instead look into the future, and for that reason, reject all three of these proposals.

256. Compare Michael W. Price, *Rethinking Privacy: Fourth Amendment Papers and the Third-Party Doctrine*, 8 J. NAT'L SEC. L. & POL'Y 247, 283 (2016) (analyzing text messages and direct social media messages under the Fourth Amendment and applying a modern-day-equivalent analysis), with Marc McAllister, *The Fourth Amendment and New Technologies: The Misapplication of Analogical Reasoning*, 36 S. ILL. U. L.J. 475, 504–05 (2012) (analyzing text messages under the Fourth Amendment and rejecting a modern-day-equivalent analysis). See Robin Miller, Annotation, *Expectation of Privacy in Text Transmissions to or from Pager, Cellular Telephone, or Other Wireless Personal Communications Device*, 25 A.L.R. 6th 201 (2007) (aggregating pre-*Carpenter* Fourth Amendment cases about text messages).

257. *Riley v. California*, 134 S. Ct. 2473 (2014).

258. *Id.* at 2488; *Carpenter v. United States*, 138 S. Ct. 2206, 2219 (2018).

A. Rejecting Conventional Analogies

In *Riley*, the Chief Justice famously and dismissively said:

The United States asserts that a search of all data stored on a cell phone is “materially indistinguishable” from searches of these sorts of physical items [such as billfolds, address books, purses, and wallets]. That is like saying a ride on horseback is materially indistinguishable from a flight to the moon. Both are ways of getting from point A to point B, but little else justifies lumping them together.²⁵⁹

This is a surprising, wholesale rejection of a conventional analogy: the government urged the Court to compare a digital technology to a physical world precursor, and the Court not only refused to do so but responded with sarcastic exaggeration. Understanding this quote is the key to understanding both *Riley* and *Carpenter* and, more broadly, the key to understanding how profoundly these cases have transformed the way the Court will reason through Fourth Amendment cases.

The horseback quote is only the most extreme example of the Court refusing to draw an analogy to an ordinary, physical world item or activity. The Court similarly dispenses with many other traditional analogies: a search through a cell phone is not like rifling through pockets;²⁶⁰ the term “cell phone” itself is misleading, because these are “minicomputers that also happen to have the capacity to be used as a telephone”;²⁶¹ and accessing CSLI is nothing like tailing a car.²⁶²

The Court did embrace some analogies in these opinions, but these tended to feel far more fanciful than the ones it rejected, drawn essentially from science fiction rather than conventional reality. Cell phones might be mistaken by aliens to be “features of human anatomy”;²⁶³ tracking CSLI is akin to “attaching an ankle monitor to the phone’s user”;²⁶⁴ searching through a cell phone is more invasive than searching through a house.²⁶⁵

Legal scholars have long analyzed the critical role of reasoning by analogy to legal reasoning.²⁶⁶ Judges decide cases by determining

259. *Riley*, 134 S. Ct. at 2488 (citations omitted).

260. *Id.* at 2484, 2489.

261. *Id.* at 2489.

262. *Carpenter*, 138 S. Ct. at 2218.

263. *Riley*, 134 S. Ct. at 2484.

264. *Carpenter*, 138 S. Ct. at 2218.

265. *Riley*, 134 S. Ct. at 2490–91.

266. See, e.g., EDWARD H. LEVI, AN INTRODUCTION TO LEGAL REASONING (2d ed. 2013); LLOYD L. WEINREB, LEGAL REASON: THE USE OF ANALOGY IN LEGAL ARGUMENT (2005); Cass R. Sunstein, *On Analogical Reasoning*, 106 HARV. L. REV. 741 (1993); Frederick

whether new fact pattern X is similar to previously analyzed fact pattern Y in relevant respects.²⁶⁷ Analogical reasoning gains force in legal reasoning because it is the “usual form of reasoning in daily life.”²⁶⁸

In Fourth Amendment jurisprudence, analogies play a dominant role. Tracking beepers are like following a car on city streets;²⁶⁹ hidden microphones are like human memory;²⁷⁰ and pen registers are like human telephone operators.²⁷¹ The *Carpenter* Court’s rejection of conventional analogies is thus a significant development. By refusing to credit the government’s preferred analogies, the Court could distinguish *Smith* and *Miller* without needing to overturn the forty-year-old precedents.

How *Carpenter* and *Riley* have treated analogy and precedent might be their most important and lasting revolution. The Court seems to be signaling that a foundation stone of legal reasoning — drawing comparisons to the ordinary, physical stuff of life — can be called into question. We are all now living in a science fictional universe, at least when making arguments to the Court. Why has the Court made this move, is it justified, and what does it mean for Fourth Amendment law going forward?

B. The Chief Justice’s Tech Exceptionalism

What causes these analogies to fail, in the eyes of the Court, is the nature of the technological era in which we are living. The Chief Justice has declared in successive landmark decisions that the information age has produced technological changes that are different in kind not merely in degree from the technology of the past.²⁷² He first announced this worldview, writing for eight justices, in *Riley v. California*, which held that the police need a warrant to search the contents of a cell phone incident to a valid arrest.²⁷³ In *Carpenter*, he exhibits the same beliefs, this time to even more consequential doctrinal import.

Schauer, *Analogy in the Supreme Court: Lozman v. City of Riviera Beach, Florida*, 2013 SUP. CT. REV. 405, 407 (2014).

267. Sunstein, *supra* note 266, at 745.

268. *Id.* at 743.

269. *United States v. Knotts*, 460 U.S. 276, 285 (1983) (comparing the use of a tracking beeper to following a suspect in a police car).

270. *United States v. White*, 401 U.S. 745, 751 (1971) (comparing a hidden microphone to an informant who writes down what he has heard).

271. *Smith v. Maryland*, 442 U.S. 735, 744 (1979) (comparing automatic telephone switching information to a human operator).

272. *See, e.g., Riley v. California*, 134 S. Ct. 2473, 2488 (2014) (“The United States asserts that a search of all data stored on a cell phone is ‘materially indistinguishable’ from searches of these sorts of physical items. That is like saying a ride on horseback is materially indistinguishable from a flight to the moon.”).

273. *Id.* at 2485.

The Chief Justice writes these opinions with what feels to me like a palpable, wide-eyed amazement at the speed with which the power and scale of technology has changed. In *Riley*, he marvels that in the five short years from arrest to Supreme Court ruling, the world had rendered obsolete the flip phone used by one of the defendants in the cases being reviewed.²⁷⁴ Similarly, in *Carpenter* he compares with astonishment the costly task of tracking a person's location on foot to the efficiency of doing so by downloading their CSLI.²⁷⁵

He emphasizes the sheer scale of modern technology. These opinions are replete with mentions of the word “millions” — “millions of pages of text;”²⁷⁶ “over a million apps available;”²⁷⁷ “396 million cell phone service accounts in the United States — for a nation of 326 million people”;²⁷⁸ and a database automatically tracking the location of “400 million devices.”²⁷⁹

Some of the words and phrases used in these opinions would seem more at home in science fiction than the U.S. Reports. These opinions invoke time travel,²⁸⁰ space travel,²⁸¹ and visits from Martians.²⁸²

The Chief Justice is equally impressed with the social dynamics of technological change — the rate with which technology like the smartphone has been adopted by Americans and has shaped our social interactions. In both opinions, he cites statistics and surveys demonstrating the large percentage of Americans who use these devices.²⁸³ He punctuates both with a statistic that has clearly left a lasting impression: “12% [of smartphone owners] admit[] that they even use their phones in the shower.”²⁸⁴

The Chief Justice connects this tech exceptionalism into Fourth Amendment doctrine with this key move: the “[m]odern cell phones are not just another technological convenience. With all they contain and all they may reveal, they hold for many Americans, the privacies of

274. *Id.* at 2484.

275. *Carpenter v. United States*, 138 S. Ct. 2206, 2217–18 (2018).

276. *Riley*, 134 S. Ct. at 2489.

277. *Id.* at 2490.

278. *Carpenter*, 138 S. Ct. at 2211.

279. *Id.* at 2218.

280. *Id.*

281. *Riley*, 134 S. Ct. at 2488.

282. *Id.* at 2484.

283. *Id.* at 2490 (citing statistic that 90% of American adults who own a cell phone use it to store private documents); *Carpenter*, 138 S. Ct. at 2211 (noting that Americans own 396 million cell phones, meaning more devices than people).

284. *Riley*, 134 S. Ct. at 2490 (citing HARRIS INTERACTIVE, 2013 MOBILE CONSUMER HABITS STUDY (2013), <https://web.archive.org/web/20130715020841/http://www.jumio.com/2013/07/where-do-you-take-your-phone/>); *Carpenter*, 138 S. Ct. at 2218. Do these people simply use their phone next to their shower to listen to audio inside the shower, or are they wrapping their device in a waterproof pouch and bringing it in with them? The Chief Justice does not say.

life.”²⁸⁵ Nothing that has come before can compare to these devices for the amount and variety of sensitive and intimate information about individuals.²⁸⁶ In the passage perhaps most bristling with constitutional import in these opinions, the Chief Justice declares that a person’s privacy interest in the contents of a smartphone is more significant than the privacy interest in a home, the ancient, paradigmatic high-water mark for privacy.²⁸⁷

What flows directly from the conclusion that these devices are unprecedented vessels for sensitive information is the recognition that technology has significantly increased the power of the police.²⁸⁸ Keeping with the science fiction theme, these devices and the records they produce essentially transform the police into crime-fighting robots outfitted with superhuman powers. They can peer into the past, avoiding the “frailties of recollection.”²⁸⁹ They can tail every suspect “every moment of every day for five years.”²⁹⁰ They are “tireless,”²⁹¹ “ever alert, and their memory is nearly infallible.”²⁹²

All of this powerful rhetoric about the power of technology has a profound impact on the reasoning of the Court by allowing it to discard analogies to what have come before. For an institution that places historical continuity, *stare decisis*, and analogical reasoning at its core, the Court’s recent refusals to accept straightforward analogies is jarring.

C. The Argument for Tech Exceptionalism

The Court’s adoption of tech exceptionalism is not science fiction; it is well justified. Changes in technology in recent years have posed challenges to privacy that are different in kind not merely in degree than what has come before. Advances in the past two decades, in particular, have dramatically decreased the ability with which individuals can understand, much less control, the ways they are observed and even controlled.

Ryan Calo has written about the tech exceptionalism of our time.²⁹³ He argues that the field of cyberlaw is premised on the idea that fundamental advances in technology such as the Internet or robotics are so qualitatively and quantitatively different from what has come before

285. *Riley*, 134 S. Ct. at 2494–95.

286. *Id.* at 2489–90.

287. *Id.* at 2491 (“[I]t also contains a broad array of private information never found in a home in any form — unless the phone is.”).

288. Kerr, *Equilibrium*, *supra* note 73, at 480.

289. *Carpenter v. United States*, 138 S. Ct. 2206, 2218 (2018).

290. *Id.*

291. *Id.*

292. *Id.* at 2219.

293. Ryan Calo, *Robotics and the Lessons of Cyberlaw*, 103 CALIF. L. REV. 513, 550–51 (2015).

that they force changes in the law.²⁹⁴ Specifically, “a technology is exceptional when its introduction into the mainstream requires a systematic change to the law or legal institutions in order to reproduce, or if necessary displace, an existing balance of values.”²⁹⁵ This is precisely what the Chief Justice argued that the smartphone and CSLI have wrought.

The Chief Justice’s arguments are backed by two decades of scholarly writing. This is perhaps best seen in the output of the annual Privacy Law Scholars Conference (“PLSC”), now in its twelfth year.²⁹⁶ The authors attending this conference have presented almost six hundred articles, the vast majority of which have argued that specific changes in technology have threatened information privacy.²⁹⁷

Articles presented at PLSC establish that technological advances increase the quantity and quality of information available to third parties.²⁹⁸ They highlight the role inference plays in disrupting settled expectations of privacy, because it is no longer enough to look at what is literally in the data;²⁹⁹ advances in technology such as machine learning give individuals the power to learn more than what is on the surface.³⁰⁰

PLSC articles have documented how these advances consistently thwart expectations and put pressure on social norms.³⁰¹ A massive literature chronicles the harms that these incursions into privacy have wrought, either on individuals, groups, or institutions.³⁰² Many articles have identified harms that go beyond traditional injury to harms that interfere with autonomy and personal development.³⁰³ Other articles discuss the futility of self-help techniques for addressing these risks.³⁰⁴

294. *Id.* at 553–58.

295. *Id.* at 552.

296. 2018 Privacy Law Scholars Conference (PLSC2018), BERKELEY LAW, <https://www.law.berkeley.edu/research/bclt/bcltevents/2018annual-privacy-law-scholars-conference> [https://perma.cc/DXK8-BFAE].

297. Data on file with author.

298. See, e.g., DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE 213 (2006).

299. Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701, 1703–04 (2010).

300. Steven M. Bellovin et. al., *When Enough Is Enough: Location Tracking, Mosaic Theory, and Machine Learning*, 8 NYU J.L. & LIBERTY 556, 560 (2014).

301. See, e.g., HELEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE (2009).

302. Daniel J. Solove & Danielle Keats Citron, *Risk and Anxiety: A Theory of Data-Breach Harms*, 96 TEX. L. REV. 737, 739 (2018); M. Ryan Calo, *The Boundaries of Privacy Harm*, 86 IND. L.J. 1131, 1133 (2011); Ohm, *Sensitive Information*, *supra* note 87, at 1196.

303. JULIE E. COHEN, CONFIGURING THE NETWORKED SELF: LAW, CODE, AND THE PLAY OF EVERYDAY PRACTICE 223–25 (2012); Neil M. Richards, *Intellectual Privacy*, 87 TEX. L. REV. 387, 389 (2008); Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609, 1613 (1999).

304. Daniel J. Solove, *Introduction: Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1879, 1880–81 (2013); see Aleecia M. McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, 4 I/S: J. L. & POL’Y FOR INFO. SOC’Y 543, 564 (2008).

It is fair to say that almost no scholarly writing refutes the argument that recent changes in technology have put significant pressure on privacy and privacy law. The very small number of detractors or skeptics who write in the field tend to argue instead that the harms are either poorly supported by empirics or outweighed by the harm that would be caused by changes to the law.³⁰⁵

Thus, Chief Justice Roberts's adoption of tech exceptionalism finds support from a significant body of scholarly argument. Far from being just the unfounded opinion of a sixty-something jurist,³⁰⁶ tech exceptionalism is an argument well within the mainstream of contemporary academic writing in privacy law.

D. Expertise and Analogy

Having established that Chief Justice Roberts views modern technology as exceptional, and having defended this view, I ask, how does this view lead him to disregard analogy and break with the Court's precedents? How does tech exceptionalism change Fourth Amendment jurisprudence? When tech exceptionalism collides with the legal system, it creates a fundamental problem of expertise. Non-technical lawyers are simply not trained to explicate the ways in which fundamental changes in complex technology put pressure on privacy and increase government power.³⁰⁷ They need to seek help from outside experts. This is especially necessary when the complex technology continues to change, presenting not only a complex target of analysis, but a moving one.

This leaves the Court needing to turn to unusual sources of technological explication.³⁰⁸ *Riley* cites multiple amici briefs for complex details about technology that were never entered into the lower court

305. Lior Jacob Strahilevitz, *Privacy Versus Antidiscrimination*, 75 U. CHI. L. REV. 363, 364 (2008); Adam Thierer, *Privacy Law's Precautionary Principle Problem*, 66 ME. L. REV. 467, 468 (2014); Eugene Volokh, *Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People from Speaking About You*, 52 STAN. L. REV. 1049, 1049 (2000); Jane Yakowitz, *Tragedy of the Data Commons*, 25 HARV. J.L. & TECH. 1, 3–4 (2011).

306. Strahilevitz, *Ten Thoughts*, *supra* note 2 (“The majority text and approach are consistent with the Chief’s dim views about legal scholarship generally and with his stated preference for minimalist decisions.”).

307. See Calo, *supra* note 293, at 560 (describing the “tradition of melding legal and technical expertise” in Cyberlaw).

308. Milligan, *supra* note 69, at 1336–37 (arguing that public interest groups and litigants should educate courts when simple analogies fail).

record.³⁰⁹ It cites to reports by government agencies known for objective scientific expertise.³¹⁰ It also contains what is probably the first Supreme Court citation ever to a smartphone operating system manual.³¹¹

Carpenter cites fewer external sources for technological facts than *Riley*, in part because it can cite *Riley* for some of its facts.³¹² Still, the majority opinion's only citation to an amicus brief is to one authored by digital civil rights groups, including the Electronic Frontier Foundation, which provides critical information about the improved precision of cell tower tracking techniques since the facts of the case were first established.³¹³

Tech exceptionalism's expertise problem explains and justifies the Court's rejection of the simplistic, conventional analogies offered by the government in *Riley* and *Carpenter*, such as the refusal to compare a smartphone to an address book.³¹⁴ In order to make proper sense of an analogy comparing an old X to a new Y, one must be expert enough to understand the relevant similarities and differences between X and Y.

This connection between analogy and expertise has been explored by legal scholars to support the argument that lawyers can sometimes see analogies that non-lawyers cannot. Frederick Schauer and Barbara Spellman offer one account.³¹⁵ A lawyer who specializes in First Amendment doctrine can see instantly the relevant similarities between self-described "Nazis" in the National Socialist Party of America and "civil rights demonstrators of the 1960s," a comparison the non-lawyer might see as "bizarre, even offensive."³¹⁶ The domain-specific expertise of First Amendment law makes apparent the similarities of these

309. *Riley v. California*, 134 S. Ct. 2473, 2486 (2014) (citing Brief of United States as amicus curiae about unbreakability of iPhone encryption); *id.* at 2487 (citing Brief for Criminal Law Professors about law enforcement use of "Faraday bags"); *id.* at 2489 (citing Brief for Center for Democracy & Technology about amount of physical world document equivalent to 16 gigabytes of digital storage); *id.* at 2490 (citing Brief for Electronic Privacy Information Center about number of smartphone apps installed by the average user).

310. *Id.* at 2486 (citing report by National Institute for Standards and Technology); *id.* at 2487 (citing report by National Institute of Justice).

311. *Id.* at 2487 (citing iPhone User Guide for iOS 7.1 Software 10 (2014)).

312. See *Carpenter v. United States*, 138 S. Ct. 2206, 2214 (2018) (citing *Riley*, 134 S. Ct. 2473, about "'immense storage capacity' of modern cell phones"); *id.* at 2218 (citing *Riley*, 134 S. Ct. 2473, for cell phone ownership and use statistics).

313. See *id.* at 2219 ("[W]ith new technology measuring the time and angle of signals hitting their towers, wireless carriers already have the capability to pinpoint a phone's location within 50 meters.") (citing Brief for Electronic Frontier Foundation et al.).

314. McAllister, *supra* note 256, at 475, 477 ("In rejecting Fourth Amendment claims involving warrantless use of sophisticated technologies, courts often rely upon analogies to prior 'search' cases, but these supposed analogies are so far removed from the new forms of surveillance that analogies to them only confuse, rather than clarify, the actual analysis required by Katz." (sic)).

315. Frederick Schauer & Barbara A. Spellman, *Analogy, Expertise, and Experience*, 84 U. CHI. L. REV. 249, 264–65 (2017).

316. *Id.* at 264–65.

groups whose wish to march in public places was opposed by viewpoint-based laws.³¹⁷

Tech exceptionalism turns the tables on lawyers, relegating them to the role of non-experts who cannot understand the failure of a given analogy because they cannot accurately characterize Y or compare it to X when complicated technology is involved.³¹⁸ Luke Milligan argues that when faced with complex technology in surveillance cases, courts should deploy an “analogy breaker” rejecting misleading analogies in favor of a “fresh ‘default’ analysis.”³¹⁹

The challenge for criminal lawyers and scholars going forward is to grapple with the nuances of technology. The Court now places great emphasis on the subtle intricacies of how technology operates, and how it differs in important ways from what has come before. We need to look to computer scientists and engineers to serve as experts and to write legal scholarship to help guide the way.³²⁰ But this is not simply a scientific or engineering exercise; the Court cares also about how humans and groups use technology. This gives impetus on new interdisciplinary bridges between law and fields such as Science and Technology Studies and Human-Computer Interaction.³²¹

The Court’s new focus on the legitimate and appropriate sources of facts should spur some modest institutional changes. Both prosecutors and defense lawyers now need sophisticated technological support, either in the form of dedicated technologists or, at the very least, hybrid-trained lawyers with some experience in technology. Civil liberties groups will need to continue their trend of hiring in-house technologists. It is not a coincidence that many of the amici briefs cited by the Court were authored by groups focused on digital civil rights and well known for hiring and associating with trained technologists.³²²

Finally, this shift should encourage legal scholars who write about the Fourth Amendment and technology to place a premium on getting

317. *Id.*

318. *See id.* at 266–67 (arguing that the domain-specific knowledge of experts allows them to see analogies that non-experts do not).

319. Milligan, *supra* note 69, at 1334–35. Milligan weighs this proposal down with concepts of “mono-analogical” and “poly-analogical” features of comparisons. *Id.* at 1324–35. Although I do not find these to be useful additions to the theory, Milligan’s bottom line is that courts should not rely too heavily on simplistic analogies when dealing with emerging technologies.

320. *See* Calo, *supra* note 293, at 561 (“Whether at conferences or hearings, in papers or in draft legislation, the legally and technically savvy will need to be in constant conversation.”).

321. *See generally* SERGIO SISMONDO, AN INTRODUCTION TO SCIENCE AND TECHNOLOGY STUDIES (2d ed. 2010); JEFF JOHNSON, DESIGNING WITH THE MIND IN MIND: SIMPLE GUIDE TO UNDERSTANDING USER INTERFACE DESIGN RULES (1st ed. 2010).

322. *See* *Riley v. California*, 134 S. Ct. 2473, 2489 (2014) (citing Brief for Center for Democracy & Technology et al.); *id.* at 2490 (citing Brief for Electronic Privacy Information Center et al.); *Carpenter v. United States*, 138 S. Ct. 2206, 2219 (2018) (citing Brief for Electronic Frontier Foundation et al.).

the technological details right. The only law review article cited in either majority opinion was authored by Orin Kerr, who is not only a preeminent scholar but also one with formal technological training and experience;³²³ and many of the majority's arguments echo themes found in uncited articles, also written by trained or technologically sophisticated legal scholars.³²⁴

E. Time and Technological Change

The unprecedented, rapidly changing nature of technology also causes the Court to relax its rules about restricting its attention to the record evidence before it. Traditionally, appellate courts, including the Supreme Court, refuse to peek outside the record developed in the trial court. Some of this reticence comes from Article III of the Constitution, which limits federal courts to consider only "cases" or "controversies."³²⁵ But it also reflects an institutional modesty that recognizes that appellate courts are distant from the facts.

Tech exceptionalism puts pressure on this understanding. The premise of tech exceptionalism is that technology changes today at unprecedented rates. An appellate court that looks only to the past is using the outdated examples in the record to set rules for the present and future, which might already differ in important ways. In *Carpenter* and *Riley*, the Court refused to resign itself to this fate. Instead, it relaxed, just slightly, its practices by peeking a little at the present and the future.

This leads to three new principles of judicial fact-finding: refresh what has changed during the pendency of litigation and appeal; relax the rules of judicial notice; and understand that the future is ascertainable.

First, the Court in these opinions shows a willingness to refresh the record, a little, at each stage of appeal. It takes several years to proceed from an arrest, through appeals, to review by the Supreme Court.³²⁶ Given the rate of change of technology, the passage of time means the Court will often be reviewing historical relics in cases like these. The

323. See *Riley*, 134 S. Ct. at 2489 (citing Orin Kerr, *Foreword: Account for Technological Change*, 36 HARV. J.L. & PUB. POL'Y 403, 404–05 (2013)). Professor Kerr has undergraduate and graduate degrees in engineering. Curriculum Vitae of Orin S. Kerr, USC GOULD, https://gould.usc.edu/portal/directory/photos/Kerr_Orin_CV.pdf [https://perma.cc/JZJ7-JYRT].

324. See, e.g., Kevin S. Bankston & Ashkan Soltani, *supra* note 70, at 335; Freiwald, *First Principles*, *supra* note 33; Henderson, *supra* note 63.

325. U.S. CONST. art. III, § 2.

326. In *Riley*, the defendants in the two cases reviewed were arrested in August 2009 and September 2007, respectively. Petition for Writ of Certiorari at 1–2, *Riley*, 134 S. Ct. 2473 (No. 13-132); *United States v. Wurie*, 728 F.3d 1, 1–2 (1st Cir. 2013). The Supreme Court decided the cases on June 25, 2014, almost five and seven years after the arrests, respectively. *Riley*, 134 S. Ct. at 2473. In *Carpenter*, the first co-conspirators were arrested in April 2011, *United States v. Carpenter*, 819 F.3d 880, 884 (6th Cir. 2016), seven years before the Supreme Court's decision. *Carpenter*, 138 S. Ct. at 2206.

Court has responded by seeing fit to peek at the present, availing itself of the kind of unusual sources of information listed above, including amici.

Second, the Court also seems willing to relax its ordinary attitudes about taking judicial notice. In *Riley*, the Court cited the iPhone User Guide for the proposition that “most phones lock at the touch of a button or, as a default, after some very short period of inactivity,”³²⁷ a citation criticized by observers.³²⁸ This extra-record “fact” was introduced to the Court through an amici brief filed by the United States in support of the State of California.³²⁹ Although the Court does not explicitly acknowledge that it is taking judicial notice³³⁰ of this technological fact, this seems to be what it has done.

Finally, the Court is not afraid to look past the facts of the technology at issue before it to the present and likely near-future technology that we will soon encounter. The Court implies that the future is ascertainable; it is something we can talk about and predict with some certainty. In *Carpenter*, the Court assessed how cell-site technology had changed in the intervening seven years.³³¹ In *Riley*, the Court noted how the flip phone at issue had already “faded in popularity.”³³²

This sets up a rather stark departure from Justice Kennedy’s approach in *City of Ontario v. Quon*,³³³ a 2010 opinion that held that a government employer’s review of an employee’s text messages on a work pager was reasonable.³³⁴ Justice Kennedy cautioned that the Court “risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear.”³³⁵ In *Carpenter*, Chief Justice Roberts prefers the *Kyllo* attitude toward predicting the future: we “must take account of more sophisticated systems that are already in use or in development.”³³⁶

327. *Riley*, 134 S. Ct. at 2487.

328. See, e.g., H. Adam Shapiro, *Court Continues to Misunderstand How We Use Technology*, DANZINGER, SHAPIRO & LEAVITT BLOG (June 25, 2014), <https://www.ds-l.com/blog/2014/06/the-supreme-court-continued-it.html> [<https://perma.cc/4G3L-Y3GK>].

329. See Brief for the United States as Amici Curiae Supporting Respondent at 11, *Riley*, 134 S. Ct. 2473 (No. 13-132), 2014 WL 1389032.

330. See FED. R. EVID. 201 (allowing federal courts to take judicial notice of facts that “can be accurately and readily determined from sources whose accuracy cannot reasonably be questioned”).

331. *Carpenter*, 138 S. Ct. at 2219 (noting how more cell towers and better technology had brought the accuracy of CSLI closer to that of GPS).

332. *Riley*, 134 S. Ct. at 2484.

333. 560 U.S. 746 (2010).

334. *Id.* at 761.

335. *Id.* at 759.

336. *Carpenter*, 138 S. Ct. at 2218–19 (quoting *Kyllo v. United States*, 533 U.S. 27, 36 (2001)).

F. Refusing to Look Backwards

The Court decided to look to the future in the face of many urging it to look to the past. Scholars urged the Court to base its Fourth Amendment decisions on a close examination of, in turn, survey evidence, history, or sources of positive law. The Court ignored all of this advice, much to the consternation of the scholars involved.

1. The Surveyors

The objective prong of the REP test asks whether an expectation of privacy is “one that society is prepared to recognize as ‘reasonable.’”³³⁷ Some have read the prong to hitch the Fourth Amendment’s protections to public sentiment.³³⁸ Police power respected the bounds of constitutional privacy so long as it did not stray too far from what ordinary people or average people expect.³³⁹ The REP test should produce results that follow, at least to some extent, what people actually expect, or so these observers have argued.³⁴⁰

For those who would connect REP to the attitudes of ordinary people, the next step was to survey Americans, gathering opinions about various police practices, including many fact patterns that have already been the subject of Supreme Court case law. This originated with landmark work in the late 1990’s by Christopher Slobogin and Joseph Schumacher.³⁴¹ Through their surveys, the pair concluded that public sentiment about the invasiveness of police practice disagreed in many instances with the Court’s Fourth Amendment doctrine.³⁴² For example, the survey respondents judged “perus[ing] bank records” to be the thirty-eighth most invasive activity out of fifty surveyed, roughly the same as “hospital surgery on shoulder,”³⁴³ contradicting the relative holdings of *Miller* and *Winston v. Lee*.³⁴⁴

The turn to survey work has been revived and invigorated in recent years.³⁴⁵ A chief advocate is Lior Strahilevitz, working with Matthew

337. *Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

338. Kugler & Strahilevitz, *Actual Expectations*, *supra* note 184, at 243.

339. *See Smith v. Maryland*, 442 U.S. 735, 740, 742 (1979).

340. *See Kugler & Strahilevitz, Actual Expectations*, *supra* note 184, at 224–25.

341. Christopher Slobogin & Joseph E. Schumacher, *Reasonable Expectations of Privacy and Autonomy in Fourth Amendment Cases: An Empirical Look at Understandings Recognized and Permitted by Society*, 42 DUKE L.J. 727, 728 (1993).

342. *Id.* at 740.

343. *Id.* at 738–40.

344. *Compare United States v. Miller*, 425 U.S. 435, 444 (1976) (holding that obtaining bank records was not a search), with *Winston v. Lee*, 470 U.S. 753, 759–63 (1985) (requiring probable cause plus additional factors for surgery in shoulder).

345. *See Bernard Chao et al., Why Courts Fail to Protect Privacy: Race, Age, Bias, and Technology*, 106 CALIF. L. REV. 263, 266 (2018); Chris Jay Hoofnagle & Jennifer M. Urban, *Alan Westin’s Privacy Homo Economicus*, 49 WAKE FOREST L. REV. 261, 262 (2014); Matthew B. Kugler & Lior Jacob Strahilevitz, *The Myth of Fourth Amendment Circularity*, 84 U.

Kugler.³⁴⁶ Strahilevitz and Kugler have written two articles reporting the results of two surveys they have conducted.³⁴⁷ The authors spend much more time than Slobogin and Schumacher trying to lay out a doctrinal and normative case for why judges ought to look to surveys when assessing police practices.³⁴⁸ They cite democratic legitimacy, doctrinal coherence and predictability, and the costs of creating legal rules that ordinary citizens don't understand or expect as the primary justifications.³⁴⁹ This work follows the broader trend in legal scholarship of finding new roles and contexts for quantitative social science.³⁵⁰

These scholars, joined by others who have published surveys about privacy attitudes, wrote an amicus brief urging the *Carpenter* Court to look to the evidence they had gathered.³⁵¹ The brief summarizes results showing that very few Americans are aware of the ability of cell phone companies to track the location of phones using CSLI, supporting an argument for requiring a warrant in the case.³⁵²

The majority opinion failed to cite any of the survey evidence in its opinion. The survey work did appear in some of the dissents, albeit in support of only minor arguments.³⁵³

Strahilevitz has been among the sharpest critics of the majority opinion's reasoning, if not its result.³⁵⁴ He faults the opinion not just

CHI. L. REV. 1747, 1751 (2017) [hereinafter Kugler & Strahilevitz, *The Myth*]; Christine S. Scott-Hayward et al., *Does Privacy Require Secrecy? Societal Expectations of Privacy in the Digital Age*, 43 AM. J. CRIM. L. 19, 22 (2015); Kugler & Strahilevitz, *Actual Expectations*, *supra* note 184, at 245; Matthew Tokson, *Knowledge and Fourth Amendment Privacy*, 111 NW. U. L. REV. 139, 144 (2016).

346. See Kugler & Strahilevitz, *The Myth*, *supra* note 345; Kugler & Strahilevitz, *Actual Expectations*, *supra* note 184.

347. Kugler & Strahilevitz, *The Myth*, *supra* note 345; Kugler & Strahilevitz, *Actual Expectations*, *supra* note 184.

348. See Kugler & Strahilevitz, *Actual Expectations*, *supra* note 184, at 224–27.

349. *Id.*

350. See Lee Epstein & Gary King, *The Rules of Inference*, 69 U. CHI. L. REV. 1, 3 (2002). Strahilevitz teaches at the University of Chicago, the cradle of law and economics. His arguments for incorporating surveys into the Fourth Amendment expressly rely on principles from law and economics. See Kugler & Strahilevitz, *Actual Expectations*, *supra* note 184, at 227 (advocating a normative framework for the Fourth Amendment that “enhance[s] social welfare” and does not spur people to “take excessive precautions to protect their information”); *id.* (“[W]e think there is a strong case to be made that misalignment between the law and societal expectations is detrimental for both efficiency and fairness-related reasons.”).

351. Brief for Empirical Fourth Amendment Scholars as Amici Curiae Supporting Petitioner, *Carpenter v. United States*, 138 S. Ct. 2206 (2018) (No. 16-402), 2017 WL 3530963.

352. *Id.* at *3 (citing study showing that only 26.5% of American cell phone users expressed even a general awareness about location tracking by cell phone companies).

353. *Carpenter v. United States*, 138 S. Ct. 2206, 2244 n.10 (2018) (Thomas, J., dissenting) (citing Kugler & Strahilevitz, *Actual Expectations*, *supra* note 184, at 241, among others, to demonstrate scholarly disapproval of the *Katz* test); *id.* at 2265 (Gorsuch, J., dissenting) (citing Slobogin & Schumacher, *supra* note 341, at 732, 740–42 for proposition that “judicial judgments often fail to reflect public views”).

354. See Strahilevitz, *Ten Thoughts*, *supra* note 2.

for failing to cite survey work but for more broadly refusing to engage legal scholarship.³⁵⁵

2. The Legal Historians

One notable legal historian who has focused on the Fourth Amendment in recent years is Laura Donohue, who has advocated for what might be described as an expansive originalism for the Fourth Amendment.³⁵⁶ In her carefully researched, book-length article, Donohue excavates English and colonial law, as well as the story of the drafting of the Constitution and Bill of Rights, to take on misimpressions of Fourth Amendment history.³⁵⁷

Professor Donohue also joined an amicus brief in *Carpenter* that was filed by a group of “scholars of the history and original meaning of the Fourth Amendment.”³⁵⁸ The historians argued that rummaging through CSLI fits the meaning of the word “search” at the time of the founding and analogized the search of CSLI as akin to the use of general warrants that motivated the Revolution and the drafters of the Bill of Rights.³⁵⁹ They noted how the early, celebrated cases of *Wilkes v. Wood*³⁶⁰ and *Entick v. Carrington*³⁶¹ involved opinions that focused on how searches created invasions into privacy and personal affairs.³⁶²

The majority opinion engages in almost no historical analysis, beyond an obligatory acknowledgement of the role the opposition to general warrants and writs of assistance played in sparking the American Revolution.³⁶³ Justices Thomas and Gorsuch engaged the history much more deeply in their respective dissents. Only Justice Thomas cites the work of legal historians, including Donohue and Cuddihy, while using the history to conclude that no search had occurred in this case — the opposite conclusion the historians pressed in their brief.³⁶⁴

355. *Id.*

356. See Laura K. Donohue, *The Original Fourth Amendment*, 83 U. CHI. L. REV. 1181, 1193 (2016).

357. *Id.* at 1193–95.

358. Brief for Scholars of the History and Original Meaning of the Fourth Amendment as Amici Curiae Supporting Petitioner, *Carpenter v. United States*, 138 S. Ct. 2206 (2018) (No. 16-402), 2017 WL 3530961. Among the other signers of the historians’ brief was William Cuddihy, author of a well cited, exhaustive history of the Fourth Amendment. See WILLIAM J. CUDDIHY, *THE FOURTH AMENDMENT: ORIGINS AND ORIGINAL MEANING* (2009).

359. Brief for Scholars, *supra* note 358, at 3.

360. (1763) 98 Eng. Rep. 489 (PC).

361. (1765) 95 Eng. Rep. 807 (KB).

362. CUDDIHY, *supra* note 358, at 9–10.

363. *Carpenter v. United States*, 138 S. Ct. 2206, 2213 (2018).

364. *Id.* at 2243 (Thomas, J., dissenting) (citing Cuddihy and Donohue); *id.* at 2240 (citing Donohue); *id.* at 2241 (same).

3. The Positive Law Proponents

Finally, much attention has been paid to a recent law review article by William Baude and James Stern.³⁶⁵ The authors propose a dramatically simplified question to replace the REP: “have [officials] engaged in an investigative act that would be unlawful for a similarly situated private actor to perform”?³⁶⁶ If yes, a search has occurred; if not, no search has occurred.³⁶⁷ The sources of illegality would include property law — thus bearing some resemblance to Justice Scalia’s rule in *Jones* — but would go beyond to include “any prohibitory legal provisions, whether legislative, judicial, or administrative in origin, and whether classified as criminal or civil in nature.”³⁶⁸

The authors argue that confining the meaning of search to issues addressed in the positive law is better than the REP test because “[i]t is conceptually clear, theoretically sound, less subjective, more legal, and responsive both to social fact and technological change.”³⁶⁹ They connect the proposal to historical references to positive law in critiques of British search and seizure practice; the structural advantages of making Fourth Amendment law act similarly to Fifth Amendment takings jurisprudence; and the idea that judging the police by the same laws that govern us all contributes to the rule of law.³⁷⁰ Finally, they point to practical advantages, touting that it betters the REP test by being clearer, equally adaptable, and more respectful of the role of the legislature.³⁷¹

Neither Baude nor Stern signed an amicus brief, but their article was cited in the Petitioner’s opening brief.³⁷² Although the majority opinion failed to cite the article, it was cited in the dissents by both Justices Thomas and Gorsuch.³⁷³

4. Looking Forward Not Backward

The majority’s refusal to embrace surveys, legal history, or the positive law when applying the Fourth Amendment to new technology should be seen as an affirmative rejection of these proposals by five justices, rather than as indifference or an oversight. The reason, once

365. See William Baude & James Stern, *The Positive Law Model of the Fourth Amendment*, 129 HARV. L. REV. 1821 (2016).

366. *Id.* at 1825.

367. The rule would extend to seizures as well. *Id.* at 1830.

368. *Id.* at 1833.

369. *Id.* at 1888.

370. *Id.* at 1837–50.

371. *Id.* at 1850–55.

372. Brief for Petitioner at 22 n.10, 32, *Carpenter v. United States*, 138 S. Ct. 2206 (2018) (No. 16-402), 2017 WL 3575179.

373. *Carpenter v. United States*, 138 S. Ct. 2206, 2242 (2018) (Thomas, J., dissenting); *id.* at 2268 (Gorsuch, J., dissenting).

again, is tech exceptionalism. Seen through this lens, approaches that look backward in time, like these three, do not serve a useful purpose, for the focus should turn to the present and future. This is not to say that history, surveys, and positive law will never again figure into Fourth Amendment cases involving advances in information technology. But for now, the Court has turned its back on them.

Most directly, history seems the wrong tool for reasoning about these questions. Given the significant differences between CSLI tracking and the location tracking of a few decades ago, it seems especially unhelpful to wonder what the Framers would have thought about CSLI.

In *Riley* and *Carpenter*, history is invoked, but briefly and in passing. History seems useful to the modern Fourth Amendment only held at a distance and as a source of very general analogy. “The fact that technology now allows an individual to carry [a cell phone’s worth of] information in his hand does not make the information any less worthy of the protection for which the Founders fought.”³⁷⁴ The suggestion is that searching a cell phone is akin to “the reviled ‘general warrants’ and ‘writs of assistance’ of the colonial era.”³⁷⁵

The Fourth Amendment is “informed by historical understandings ‘of what was deemed an unreasonable search and seizure [when the Fourth Amendment] was adopted.’”³⁷⁶ It is meant to “secure ‘the privacies of life’ against ‘arbitrary power,’” and “a central aim of the Framers was ‘to place obstacles in the way of a too permeating police surveillance.’”³⁷⁷ These quoted passages are the sum total of the Court’s attention to history in these two landmark opinions, a far cry from what the historians had hoped to see.

The problem with survey results in an era of tech exceptionalism is that lay attitudes about rapidly changing technology are likely to be rapidly changing, unstable, and uninformed. It is one thing to look at survey results to ask whether Americans think the police ought to be able to hide a recording device on a confidential informant. Average Americans have had nearly a century to understand voice recording and millennia to have developed fixed opinions about misplaced confidences.³⁷⁸ This seems like the kind of technology-aided surveillance that a court might rely on a survey to assess. But asking average Americans to opine about cell-site location information or facial recognition or smart meters is simply not likely to produce informed opinions.³⁷⁹ At best, it will reflect still developing attitudes about misunderstood

374. *Riley v. California*, 134 S. Ct. 2473, 2495 (2014).

375. *Id.* at 2494.

376. *Carpenter*, 138 S. Ct. at 2214.

377. *Id.*

378. See, e.g., CUDDIHY, *supra* note 355, at 333 (discussing use of informants for securing warrants in the colonies).

379. See Freiwald, *First Principles*, *supra* note 33, at *25.

and changing technologies. To be fair, Strahilevitz suggests something similar in his work.³⁸⁰ Why we would hitch our constitutionally bestowed civil liberties to the quicksand of the median American's technology literacy defies common sense.

The situation for the positive law is even worse. It compounds the confusion the general public has about the social meaning of rapidly changing technology with the vagaries of the sclerotic legislative and judicial processes.³⁸¹ This is especially true when considering statutory privacy law. Many have decried the state of privacy legislation at the national and state levels today as failing properly to account for the harms that can be wrought by new technology.³⁸² The situation has become much worse in recent years, as technology companies have discovered Washington and today spend more than almost any industry lobbying Congress.³⁸³

To put it succinctly, applying the Fourth Amendment to information technology requires the Court to look forward; all three of the proposed approaches look backward instead.

V. CONCLUSION

Based on the new rule it announces, *Carpenter* is already on par with some of the most consequential Fourth Amendment cases of all time. But when one looks beyond the core rule to some of the other revolutions wrought in the opinion, one is left to conclude that *Carpenter* represents a fundamental shift, not merely an incremental adaptation. *Carpenter* turns the third-party doctrine inside out, eroding the requirement of government action as a core underpinning of the Fourth Amendment; it applies even when the government acts directly to collect information about many individuals in massive databases; it implicitly suggests three new rules of technological equivalence; it embraces a tech exceptionalism that permits a break from judicial precedent; and it begins the overdue project of replacing the *Katz* REP test.

380. Kugler & Strahilevitz, *Actual Expectations*, *supra* note 184, at 234–35 (“We do think that the case for placing real weight on survey responses is strongest when laypeople are being surveyed on issues that are familiar to them. For that reason, our surveys ask people about the sorts of technologies that they are likely to have encountered in the world . . .”).

381. See Richard M. Re, *The Positive Law Floor*, 129 HARV. L. REV. F. 313, 326–27 (2016) (critiquing the positive law model by pointing to many reasons legislatures might not have yet regulated a new technology, including “regulatory lag”).

382. See, e.g., Ohm, *Sensitive Information*, *supra* note 87, at 1127.

383. See Re, *supra* note 381, at 329 (discussing role of private interest groups in debates surrounding legislation regulating privacy in data); see also OPENSECRETS.ORG, 2017 TOP INDUSTRIES, <https://www.opensecrets.org/lobby/top.php?indexType=i&showYear=2017> [<https://perma.cc/QCF2-FSS8>].

On December 19, 1967, the day after the Court decided *Katz*, it probably was not yet clear what the Court had done.³⁸⁴ The decision was rightly seen as important, the culmination of almost forty years of scholarly commentary against the narrow trespass theory reasoning of *Olmstead v. United States*.³⁸⁵ What might have been seen at first as merely an important decision only later was rightfully recognized for the many revolutions it created.

What *Katz* did to *Olmstead*, *Carpenter* will do to *Katz*, transforming the Fourth Amendment into something fundamentally new. The Fourth Amendment has become the vessel for a civil right that, for the first time, responds flexibly and rapidly to the insistent challenges of new technology on privacy.

384. *Katz v. United States*, 389 U.S. 347, 347 (1967). See Anthony G. Amsterdam, *Perspectives on the Fourth Amendment*, 58 MINN. L. REV. 349, 383–85 (1974) (writing seven years after *Katz*, describing the evolution in how the case had by then been interpreted).

385. *Olmstead v. United States*, 277 U.S. 438, 568 (1928); see Winn, *supra* note 377, at 2 (“The *Olmstead* decision was very divisive, and the government’s use of wiretaps continued to be controversial.”).

From: (b)(6); (b)(7)(C)
Sent: 14 Nov 2019 13:51:16 +0000
To: (b)(6); (b)(7)(C)
Subject: RE: Venntel - Geolocation Data Services Legal Review Process

Hi (b)(6); (b)(7)(C)

(b)(5)

(b)(6); (b)(7)(C)
Acting HSILD Deputy Chief
Homeland Security Investigations Law Division
Office of the Principal Legal Advisor
U.S. Immigration and Customs Enforcement
202-732- (office)
202-494- (mobile)
(b)(6); (b)(7)(C)@ice.dhs.gov

***** WARNING *** ATTORNEY/CLIENT PRIVILEGE *** ATTORNEY WORK PRODUCT *****

This document contains confidential and/or sensitive attorney/client privileged information or attorney work product and is not for release, review, retransmission, dissemination or use by anyone other than the intended recipient. Please notify the sender if this message has been misdirected and immediately destroy all originals and copies. Any disclosure of this document must be approved by the Office of the Principal Legal Advisor, U.S. Immigration & Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY. FOIA exempt under 5 U.S.C. § 552(b)(5).

From: (b)(6); (b)(7)(C)@ice.dhs.gov>
Sent: Wednesday, November 13, 2019 6:53 PM
To: (b)(6); (b)(7)(C)@ice.dhs.gov>
Subject: RE: Venntel - Geolocation Data Services Legal Review Process

(b)(5)

Thanks, (b)(6); (b)(7)(C)

(b)(6); (b)(7)(C) **J.D./Joint M.S. Cybersecurity**
Management and Program Analyst
Office of Information Governance and Privacy, Privacy Division
U.S. Immigration and Customs Enforcement
Mobile: 401-826-(b)(6); (b)(7)(C)
PCN: (b)(6); (b)(7)(C)

From: (b)(6); (b)(7)(C)@ice.dhs.gov>
Sent: Monday, October 28, 2019 2:43 PM
To: (b)(6); (b)(7)(C)@ice.dhs.gov>
Cc: Holz, Jordan (b)(6); (b)(7)(C)@ice.dhs.gov>; (b)(6); (b)(7)(C)@ice.dhs.gov>
Subject: RE: Venntel - Geolocation Data Services Legal Review Process

Hi (b)(6); (b)(7)(C)

(b)(5); (b)(6); (b)(7)(C)

(b)(6); (b)(7)(C)
Associate Legal Advisor
Homeland Security Investigations Law Division
Office of the Principal Legal Advisor
U.S. Immigration and Customs Enforcement
202-732-(b)(6); (b)(7)(C) office)
202-494-(b)(6); (b)(7)(C) mobile)
(b)(6); (b)(7)(C)@ice.dhs.gov

***** WARNING *** ATTORNEY/CLIENT PRIVILEGE *** ATTORNEY WORK PRODUCT *****

This document contains confidential and/or sensitive attorney/client privileged information or attorney work product and is not for release, review, retransmission, dissemination or use by anyone other than the intended recipient. Please notify the sender if this message has been misdirected and immediately destroy all originals and copies. Any disclosure of this document must be approved by the Office of the Principal Legal Advisor, U.S. Immigration & Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY. FOIA exempt under 5 U.S.C. § 552(b)(5).

From: (b)(6); (b)(7)(C)@ice.dhs.gov>
Sent: Wednesday, October 23, 2019 3:57 PM
To: (b)(6); (b)(7)(C)@ice.dhs.gov>
Cc: Holz, Jordan (b)(6); (b)(7)(C)@ice.dhs.gov>; (b)(6); (b)(7)(C)@ice.dhs.gov>
Subject: Venntel - Geolocation Data Services Legal Review Process

Hi (b)(6); (b)(7)(C)

From: (b)(6); (b)(7)(C)
Sent: 14 Nov 2019 13:59:49 +0000
To: (b)(6); (b)(7)(C)
Subject: RE: Venntel - Geolocation Data Services Legal Review Process

Hi (b)(6); (b)(7)(C)

Good to know. Thanks so much, (b)(6); (b)(7)(C)

(b)(6); (b)(7)(C) **.D./Joint M.S. Cybersecurity**
Management and Program Analyst
Office of Information Governance and Privacy, Privacy Division
U.S. Immigration and Customs Enforcement
Mobile: 401-826 (b)(6); (b)(7)(C)
PCN: (b)(6); (b)(7)(C)

From: (b)(6); (b)(7)(C)@ice.dhs.gov>
Sent: Thursday, November 14, 2019 8:51 AM
To: (b)(6); (b)(7)(C)@ice.dhs.gov>
Subject: RE: Venntel - Geolocation Data Services Legal Review Process

Hi (b)(6); (b)(7)(C)

(b)(5)

(b)(6); (b)(7)(C)
Acting HSILD Deputy Chief
Homeland Security Investigations Law Division
Office of the Principal Legal Advisor
U.S. Immigration and Customs Enforcement
202-732 (b)(6); (b)(7)(C) office)
202-494 (b)(6); (b)(7)(C) mobile)
(b)(6); (b)(7)(C)@ice.dhs.gov

***** WARNING *** ATTORNEY/CLIENT PRIVILEGE *** ATTORNEY WORK PRODUCT *****

This document contains confidential and/or sensitive attorney/client privileged information or attorney work product and is not for release, review, retransmission, dissemination or use by anyone other than the intended recipient. Please notify the sender if this message has been misdirected and immediately destroy all originals and

From: (b)(6); (b)(7)(C)
Sent: 19 Nov 2019 19:59:51 +0000
To: (b)(6); (b)(7)(C) Holz, Jordan
Subject: DHS OGC Request for Information

Hi Privacy Folks,

(b)(5)

Thanks,

(b)(6); (b)(7)(C)

(b)(6); (b)(7)(C)

Acting Deputy Chief
Homeland Security Investigations Law Division
Office of the Principal Legal Advisor
U.S. Immigration and Customs Enforcement
202-732-(b)(6); (b)(7)(C) office)
202-494-(b)(6); (b)(7)(C) mobile)
(b)(6); (b)(7)(C)@ice.dhs.gov

***** WARNING *** ATTORNEY/CLIENT PRIVILEGE *** ATTORNEY WORK PRODUCT *****

This document contains confidential and/or sensitive attorney/client privileged information or attorney work product and is not for release, review, retransmission, dissemination or use by anyone other than the intended recipient. Please notify the sender if this message has been misdirected and immediately destroy all originals and copies. Any disclosure of this document must be approved by the Office of the Principal Legal Advisor, U.S. Immigration & Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY. FOIA exempt under 5 U.S.C. § 552(b)(5).

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)



(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)