THE FOURTH AMENDMENT IN A DIGITAL WORLD

*LAURA K. DONOHUE**

I. Introduction 554
II. Literal Reading of the Text 560
  A. Houses 561
  B. Papers 568
  C. Voice Communications 573
III. Private versus Public Space 581
  A. Open Fields, Naked Eye 582
  B. Aerial Surveillance 589
  C. Radio-frequency Enabled Transmitters 594
  D. Global Positioning System Technology 599
  E. Enhanced Detection 609
  F. Technological Challenges to the Private/Public Distinction 612
    1. Digital Tracking 613
    2. Recording and Analysis: Informants and the First Amendment 631
IV. Personal Information versus Third-Party Data 640
  A. Information Entrusted to Others 641
  B. Digital Dependence 647
V. Content versus Non-Content 650
  A. Electronic Communications 651
  B. Pen Register/Trap and Trace Devices 658
  C. Envelope Information 661
VI. Domestic versus International 664
  A. Law Enforcement 666
  B. Foreign Intelligence Collection 668
  C. Technological Challenges to the Domestic/International Distinction 674
VII. Confronting the Digital World 678

* Professor of Law, Georgetown Law; Director, Georgetown Center on Law and National Security; Director, Georgetown Center on Privacy & Technology. Thanks to Joel Brenner, Allegra McLeod, Matthew Waxman, and participants in the Georgetown Law Faculty Workshop for their comments on an earlier version of this Article. I also am grateful to Jeremy McCabe, who provided invaluable help in securing many of the cases, laws, texts, and papers cited in this Article.

I.
INTRODUCTION

Fourth Amendment doctrine no longer reflects how the world works. Technology has propelled us into a new era. Traits unique to a digital world are breaking down the distinctions on which the Court has traditionally relied to protect individual privacy.

What are these characteristics? Digital information is ubiquitous. Individuals cannot go about their daily lives without generating a footprint of nearly everything they do. The resulting data is accessible, recordable, and analyzable. And because it is digital, it can be combined with myriad sources, yielding deeper insight into our lives. Data is also non-terrestrial and borderless. Bits and bytes populate an alternative world. They may be held on a server, but their generation, transfer, and availability are not tied to territory, undermining doctrines that rely on three-dimensional space. Technology, moreover, embodies an efficiency drive. Innovation makes it possible to do more, and to do it better, faster, and cheaper than before. So more information is being captured, even as the resource expenditures required steadily decline. Simultaneously digital interfaces are rapidly proliferating, replacing traditional modes of interaction. This means that new types of information are available, even as our ability to conduct our daily lives has become heavily dependent on technology. It has become a non-option to eschew the digital world, if one wants to live in the modern age.

These characteristics undermine the distinctions that mark Fourth Amendment doctrine. Consider, for instance, the diremption between private and public space. The Court has long relied upon this dichotomy to determine what constitutes a reasonable expectation of privacy.[1] It draws a line at the walls of the home, citing the risk assumed by individuals when they go out into public and expressing a reluctance to disadvantage law enforcement by forcing them to turn off their natural senses or to ignore what any ordinary person could ascertain.

The amount and types of information available in the public sphere, however, have exponentially increased. WiFi and Bluetooth signals can be collected, global positioning systems and vessel monitoring systems operated, and radio frequency identification chips tracked. Automated license plate readers record the time, date, and

1. *See, e.g.*, Brief of James Otis, Paxton's Case (Mass. Sup. Ct. 24–26 Feb. 1761); Part II(A), *infra*. *Cf.* Raleigh, Opinion, 3 MASSACHUSETTS SPY, Apr. 29, 1773, at 1, cols. 1–2 (discussing the problems with royal officers seizing traders' property without "proper cause").

location of cars, while network data reveals where mobile devices travel day and night. International mobile-subscriber identity-catchers pinpoint the devices located in a given area. Internet protocol databases, in turn, register users' locations. Financial transactions and credit card records place people in certain places at certain times, while cameras, enhanced with remote biometric identification, may be mounted on vehicles, poles, buildings, or unmanned aerial systems, creating the potential for 24-hour monitoring, seven days a week, *ad infinitum*.[2]

The digitization of this information means that it can be recorded and combined with biographic information and subjected to algorithmic analyses, penetrating further into citizens' lives. Even when data is derived from the public sphere, the government's use of it may impact free speech, the right to assemble, and religious freedom, to say nothing of personal privacy.

Technology erodes other Fourth Amendment distinctions. A series of cases in the 1970s established the contours of what would be considered "reasonable," based on who holds the information. Data held by the individual generating it is afforded a higher level of protection, while data held by third parties, such as companies with whom one contracts for goods or services, is granted a lower level of protection. But technology has created an imbalance. Digital dependence—i.e., the degree to which we rely on digitization to live our daily lives—has radically changed the world in which we live.[3] School, work, social interactions, hobbies, and other pursuits are now online by nature of how society functions. This has two implications. First, new kinds of information are now generated and, therefore, accessible. Second, our reliance on industry and third-party providers to service the needs of daily life has made much more of our personal information, as well as new kinds of personal data, vulnerable to government collection.[4]

---

2. For discussion of facial recognition technologies and remote biometric identification, see Laura K. Donohue, *Technological Leap, Statutory Gap, and Constitutional Abyss: Remote Biometric Identification Comes of Age,* 97 MINN. L. REV. 407 (2012); U.S. GOV'T ACCOUNTABILITY OFFICE, GAO–15–621, FACIAL RECOGNITION TECHNOLOGY: COMMERCIAL USES, PRIVACY ISSUES, AND APPLICABLE FEDERAL LAW (2015); Mark Pomerleau, *A Closer Look at Facial Recognition*, GCN (Aug. 7, 2015), https://gcn.com/articles/2015/08/07/facial-recognition.aspx.

3. For a thoughtful, early discussion about the increasing centrality of digitization, see generally DANIEL J. SOLOVE, THE DIGITAL PERSON (2004).

4. Amazon Echo, for instance, can hear what one is saying from across a crowded room. Alyssa Newcomb, *How Amazon Echo Can Hear What You're Saying from Across the Room*, ABC NEWS (Nov. 6, 2014, 4:01 PM), http://abcnews.go.com/Technology/amazon-echo-hear-room/story?id=26740479. Samsung's own privacy

Another distinction centered on the *type* of information under consideration—content versus non-content—similarly collapses in the contemporary world. For years, envelope information has been considered non-content, and thus less protected than content, on the grounds that the latter, and not the former, reveals an individual's private communications, thoughts, and beliefs. But what happens when a search engine reveals what it is that is being examined in the uniform resource locator (URL) itself?[5] Metadata of all sorts can reveal much about an individual[6]—indeed, law enforcement regularly uses search terms to bring criminal charges against individuals. The reason is simple: patterns in phone calls, text messages, instant messaging, emails, or even URL visits demonstrate beliefs, relationships, and social networks—yet the form of that data (metadata) has not historically been considered content. The same is true of consumer metadata and financial records. Sophisticated pattern analytics mean that non-content morphs into content, making any formal distinction meaningless.[7]

---

policy for its smart televisions warns consumers that anything discussed in the proximity can be "captured and transmitted to a third party." Alyssa Newcomb, *Samsung Privacy Policy: Watch What You Say Around Your Smart TV,* ABC NEWS (Feb. 9, 2015, 9:29 AM), http://abcnews.go.com/Technology/samsung-privacy-policy-watch-smart-tv/story?id=28829387. Their televisions use facial recognition and biometric identification technologies to track family members' actions, expressions, and utterances. *See id.*; *Samsung Privacy Policy – SmartTV Supplement*, http://www.samsung.com/sg/info/privacy/smarttv.html (last visited Oct. 29, 2016). Toys inside the home similarly record private conversations. Although Fourth Amendment doctrine draws a line at the curtilage of the home, extending higher protections to what happens indoors, it simultaneously divests third party data of any privacy interest. Fourth Amendment doctrine has yet to address the tension.

5. If I were, for instance, to search for "Molotov cocktail" on Amazon.com, the URL that comes up is https://www.amazon.com/s/ref=NB_sb_noss_1?url=search-alias%3Daps&field-keywords=Molotov_cocktail. Subject-specific sites similarly indicate the content, with Wikipedia's URL reading https://en.wikipedia.org/wiki/Molotov_cocktail.

6. *See generally* Laura K. Donohue, *Bulk Metadata Collection: Statutory and Constitutional Considerations,* 37 HARV. J. L. & PUB. POL'Y 757 (2014) [hereinafter Donohue, *Bulk Metadata*] (discussing privacy issues regarding the NSA's bulk collection of telephony metadata); LAURA K. DONOHUE, THE FUTURE OF FOREIGN INTELLIGENCE 39–53 (2016) [hereinafter DONOHUE, FUTURE]. A helpful definition of "metadata" offered by Anne J. Gilliland is "the sum total of what one can say about any information object at any level of aggregation." An "information object," in turn, "is a digital item or group of items, regardless of type or format, that can be addressed or manipulated as a single object by a computer." Anne J. Gilliland, *Setting the Stage*, *in* INTRODUCTION TO METADATA 1, p.2 (Murtha Baca ed., 2d ed. 2008).

7. *See, e.g.,* Swati Agarwal et al., *Open Source Social Media Analytics for Intelligence and Security Informatics Applications*, *in* BIG DATA ANALYTICS: 4TH INTERNATIONAL

Differentiating between domestic and international communications similarly proves inapposite to the contemporary world. Communications are now global. If I email a friend from a restaurant in Boston and she reads the email while sitting at a restaurant in New York, the message may well have gone internationally, placing it under weaker Fourth Amendment standards.[8] It is not that the privacy interest in the communication is any different than that of a traditional letter. It is simply that digitization and the advent of worldwide communications networks *have narrowed my right to privacy for the same information*. Or how about cloud computing, or the use of Drop Box, or Google Docs? Is all of this information fair game, so to speak, just because Google happens to hold the document in Singapore as opposed to San Francisco? The problem, as with the distinctions between private and public space, or content and non-content, has nothing to do with the interests implicated and everything to do with new technologies.

This Article explores how digitization is challenging formal distinctions in Fourth Amendment doctrine that previously have played a role in protecting the right to privacy.[9] The purpose, consistent with the aim of the *NYU Annual Survey of American Law*, is to

---

CONFERENCE, BDA 2015, at 21, 28–30 (Naveen Kumar & Vasudha Bhatnager eds., 2015) (using YouTube metadata to identify extremists); *id.* at 30–32 (using Twitter metadata to detect hate-promoting content and predict civil unrest); Carson Kai-Sang Leung & Fan Jiang, *Big Data Analytics of Social Networks for the Discovery of "Following" Patterns*, *in* BIG DATA ANALYTICS AND KNOWLEDGE DISCOVERY, 17TH INTERNATIONAL CONFERENCE, DAWAK 2015, at 123, 126–134 (Sanjay Madria & Takahiro Hara eds., 2015) (using metadata to determine relationships between individuals in social networks).

8. For further discussion of the conditions under which the e-mail could be read for foreign intelligence purposes, see generally DONOHUE, FUTURE, *supra* note 6.

9. There are other distinctions and aspects of Fourth Amendment doctrine that this article does not consider. For instance, searches of personal devices give rise to a range of questions about the limits of plain view doctrine and ways in which such searches can be narrowed to avoid a descent into a general warrant. For a thoughtful discussion of this point, see generally Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531 (2005). The argument recurs in Orin S. Kerr, *Digital Evidence and the New Criminal Procedure*, 105 COLUM. L. REV. 279, 300 (2005). Another distinction made in the statutory realm is between stored communications and communications in transit, with the latter given more protections. Some commentators have argued that law enforcement has exploited this distinction to afford the type of digital information held by ISPs (photographs, e-mail, bank records, and medical records) a lower level of protection. *See, e.g.*, James M. O'Neil, Note, *The Impact of VoIP Technology on Fourth Amendment Protections Against Electronic Surveillance*, 12 INTELL. PROP. L. BULL. 35, 42–43 (2008). I do not address this directly in the Article as it is primarily a statutory concern.

provide an overview of where the doctrine has been and where it is now, with some thoughts about what direction it could go to take account of the privacy interests implicated by the digital world.[10]

This Article postulates that four Fourth Amendment dichotomies (private vs. public space; personal vs. third party data; content vs. non-content; and domestic vs. international) are breaking down in light of new and emerging technologies. The distinctions are becoming blurred. Information previously protected is no longer guarded. The categories themselves are failing to capture important privacy interests, so fewer protections are being granted at the outset. Simultaneously, the absence of use restrictions in Fourth Amendment doctrine blinds the law to the deeper privacy interests at stake. Legal doctrines that fail to recognize any privacy interest in the collection of information at the outset prove inadequate to acknowledge interests that later arise apparently *ex nihilo*,[11] despite the fact that more serious inroads into privacy occur with the recording of data, extended collection, and further analysis of the information. In addition, as the collection and analysis of information requires fewer and fewer resources, constraints that previously played a key role in protecting privacy are dropping away. The way in which the digital era interacts with the doctrine is steadily constricting the right to privacy. If no steps are taken to stem the tide, privacy interests will continue to narrow with significant long-term implications.

Part II of this Article begins the survey by focusing on the territorial grounding of Fourth Amendment doctrine at the founding. It describes the Court's literal, textual reading of "houses" as matters within the home, while explaining that "papers" meant that letters sent through the post received *the same protections* as items

10. The journal, which was founded in 1942, aims to provide a comprehensive summary of developments in American law. *See Mission*, N.Y.U. Annual Survey of American Law, https://annualsurveyofamericanlaw.org/aboutus/ (last visited Nov. 2, 2016).

11. *See, e.g.*, *In re* Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things from [Redacted Text], BR 13-109, at 9 (FISA Ct. Aug. 29, 2013), https://www.aclu.org/files/assets/br13-09-primary-order.pdf ("[W]here one individual does not have a Fourth Amendment interest, grouping together a large number of similarly-situated individuals cannot result in a Fourth Amendment interest springing into existence *ex nihilo*."). Some commentators have argued for a continued adherence to this approach, despite the privacy interests implicated by long-term surveillance. *See, e.g.*, Orin Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311, 353–54 (2012) (rejecting the concerns of the shadow majority in *United States v. Jones*, 132 S.Ct. 945 (2012)).

inside the home.[12] The doctrine hewed to a three-dimensional worldview. But with the advent of the telephone, the question of how to protect similar interests with regard to voice communications created difficulties.

Part III begins with *Katz v. United States*,[13] which aspired to rather more than it delivered. Even as it (ostensibly) wrenched reasonableness from a territorial tie, the Court entrenched the private/public distinction.[14] The persistence of the open fields doctrine, the establishment of aerial surveillance, and the Court's failure to acknowledge the impact of tracking technologies on personal liberty reinforced the dichotomy. Thermal scanning underscored the reliance on line-drawing in three-dimensional space. This Article focuses on location tracking to illustrate gaps in the Court's jurisprudence that result from new technologies.

Part IV turns to the distinction between personal information and third party data, noting that the constellation of cases from the 1970s similarly fails to acknowledge the ever-deepening privacy interests of a digital age. Increasing dependence on technology means that the amount of private information at stake is considerable.

Part V considers the content versus non-content dichotomy, noting that technology is blurring the distinction. Electronic communications that convey content are not currently protected, even as areas traditionally considered to fall on the non-content side of the line, such as data from pen register (or trap and trace devices) or envelope information, provide insight into individuals' private affairs.

Part VI focuses on the domestic versus international distinction. It begins by recognizing that the Fourth Amendment did not initially extend beyond the United States. In 1967, the Court changed course for U.S. persons overseas, granting limited protec-

12. Besides *Dow Chem. Co. v. United States*, 476 U.S. 227 (1986), discussed *infra*, this Article does not explore the complexity of Fourth Amendment doctrine with regard to businesses. *See, e.g.*, Minnesota v. Carter, 525 U.S. 83 (1998). For additional discussion, see, for example, Russell L. Weaver, *The Fourth Amendment, Privacy and Advancing Technology*, 80 Miss. L. J. 1131, 1162–63, 1174–77, 1202–05 (2011).

13. 389 U.S. 347 (1967).

14. *See* Weaver, *supra* note 12, at 1222 (suggesting that the post-*Katz* cases actually digressed with regard to standing doctrine, while "the Court's post-*Katz* technology decisions are a bit more of a mixed bag. However, in a number of those cases, the Court has restrictively construed the [reasonable expectation of privacy] test;" nevertheless, the author finds some "heartening trends for privacy in some recent decisions.").

tions. In 1990, it determined that non-U.S. persons located abroad and lacking a substantial connection to the U.S. hold no constitutional rights under the Fourth Amendment. This section contrasts the law enforcement approach with that adopted in the foreign intelligence realm, which similarly draws a line at the border. The problem comes in the form of new technologies, which doggedly refuse to recognize terrestrial boundaries. Domestic communications may now travel outside the country, simply by nature of how the Internet works. In so doing, they lose protections that they otherwise would have had, had they stayed within the country.

Part VII concludes by highlighting the importance of re-thinking the theoretical framing for the Fourth Amendment. While some commentators have suggested that legislation is the most appropriate vehicle to address Fourth Amendment concerns, it is to the Courts we must look to for relief. The questions posed by the digital age are profound. Failure to address them in a meaningful way will lead to continually narrower constitutional protections, at great cost to liberty in the United States.

II.
LITERAL READING OF THE TEXT

Fourth Amendment doctrine has long recognized the importance of protecting individuals within their homes from governmental intrusion. Prior to the 1970s, it afforded what people did in public, or made visible to others, considerably less protection. The doctrine reflected a literal reading of the text. The right of the people to be secure in their homes meant precisely that, just as the right to be secure in one's papers afforded special protections to correspondence. Letters inside an envelope and sent through the post obtained the same protections as papers held inside the home. Once the letters were sealed and blocked from the sight of prying eyes, the fact that they were being transmitted in the mail did not alter the underlying privacy interests. Any effort to intercept and to read such documents amounted to a search, making warrantless access presumptively unreasonable.

The rationale made sense. One knew when one entered into public space that what was said and done could be seen and heard by others. If any citizen could witness others' behavior, why should government officials, who also happened to be present, not be allowed to do the same? Similarly, one could hardly expect postal employees sorting the mail, or a postman delivering a letter, to avert their gazes from the writing on the back of a post card situated adjacent to the address. If they could see it, why shouldn't law

enforcement? A different rule applied to correspondence hidden from public view. Taking the step to open the letter altered the behavior in question and the privacy rights entailed.

The concepts on which the distinction rested (the risk assumed by individuals doing things in public, in front of other people, and the absurdity of directing people to close their eyes, avert their gazes, or otherwise ignore their senses) became intertwined. What was visible in public to others did not fall within the protections of the Fourth Amendment. In contrast, where the government wanted to intrude on the sanctity of the home, outside of exigent circumstances, it was forced to approach a judge, to present evidence, under oath, of criminal activity, and to obtain a warrant that detailed precisely what was to be searched, or who or what would be seized, from where. Similarly, if officers wanted to read a letter located in a sealed envelope, they had to first obtain a warrant.

The line was drawn in the physical world, at the border of the home, or the parchment that made up the envelope. What was inside a home or an envelope, was *de facto* private, while what occurred outside the physical bounds of the home or the envelope was, with some exceptions, generally public.

A. Houses

For centuries prior to the founding of the United States, English common law afforded individuals' homes special protections.[15] Legal treatises detailed limits that prevented officers of the Crown from entering domiciles absent sufficient cause and/or application to a magistrate, demonstrating, under oath, probable cause of criminal activity.[16] English jurists, lawyers, and Parliamen-

15. For discussion on the origins of the Fourth Amendment and its ties to English legal treatises and cases, see generally Laura K. Donohue, *The Original Fourth Amendment*, 83 U. Chi. L. Rev. 1181 (2016) [hereinafter Donohue, *Original*]. Chapter Four of Laura K. Donohue, The Future of Foreign Intelligence: Privacy and Surveillance in a Digital Age (2016) provides a broad overview of the founding generation's aim in enacting the Fourth Amendment, while Chapter Five focuses on general warrants. For purposes of this Article, citations related to the original meaning of the Fourth Amendment are to the *Chicago Law Review* article, which goes into greater detail than the book. For individuals interested in a broader overview, see generally Donohue, Future, chs. 4, 5.

16. *Id.* at 1235. In 1604, Sir Edward Coke famously proclaimed in *Semayne's Case* "[t]hat the house of everyone is to him as his castle and fortress, as well for his defence against injury and violence, as for his repose." Semayne's Case, (1604) 77 Eng. Rep. 194, 195 (K.B.), 5 Co. Rep. 91 a, 93 b. In 1628 Coke reiterated this view in his *Institutes of the Laws of England*: "[F]or a mans [sic] house is his castle, *et domus sua cuique est tutissimum refugium* [and each man's home is his safest refuge]." Sir Edward Coke, The Third Part of the Institutes on the Laws of

tarians similarly extolled the importance of protecting the home from undue government interference.[17]

ENGLAND: CONCERNING HIGH TREASON, AND OTHER PLEAS OF THE CROWN, AND CRIMINALL CASES 162 (London, M. Flesher 1648). In 1736, Sir Matthew Hale underscored the protections afforded under common law, detailing the conditions under which justices of the peace, sheriffs, constables, or watchmen could breach one's walls. *See* 2 MATTHEW HALE, THE HISTORY OF THE PLEAS OF THE CROWN 85–95 (1736); *see also* Donohue, *Original*, *supra* note 15, at 1235–36 (detailing the conditions under which the home could be breached). William Blackstone in his *Commentaries on the Laws of England*, expounded on Coke, tying the right to be secure in one's abode back to Ancient Rome:

> [T]he law of England has so particular and tender a regard to the immunity of a man's house, that it stiles it his castle, and will never suffer it to be violated with impunity: agreeing herein with the sentiments of ancient Rome, as expressed in the words of Tully; '*quid enim sanctius, quid omni religione munitius, quam domus uniuscujusque civium*?' ['For what is more sacred, what more inviolable, than the house of every citizen']

4 WILLIAM BLACKSTONE, COMMENTARIES ON THE LAWS OF ENGLAND (Clarendon 1769) 223 (footnote omitted). William Hawkins' *Pleas of the Crown* reinforced the point, citing to Hale's conditions of entry to emphasize the special place accorded to dwellings. 2 WILLIAM HAWKINS, PLEAS OF THE CROWN 139 (London, Whieldon 6th ed. 1787), https://play.google.com/store/books/details?id=2qYDAAAAQAAJ&rdid=book-2qYDAAAAQAAJ&rdot=1; *see also* Donohue, *Original*, *supra* note 15, at 1215–17 (discussing the writings of Hale and Hawkins).

17. In *Wilkes v. Wood*, an action in trespass, John Glynn argued that the case "touched the liberty of every subject of this country, and if found to be legal, would shake that most precious inheritance of Englishmen." (1763) 98 Eng. Rep. 489, 490 (C.P.); *see also* Donohue, *Original*, *supra* note 15, at 1199–1204 (discussing *Wilkes v. Wood*). Glynn protested: "In vain has our house been declared, by the law, our asylum and defence, if it is capable of being entered, upon any frivolous or no pretence at all, by a Secretary of State." *Wilkes*, 98 Eng. Rep. at 490. Commenting on the award of £1000 in damages, the *The London Chronicle* observed, "By this important decision, every Englishman has the satisfaction of seeing that his home is his castle." 14 THE LONDON CHRONICLE, 550 (Dec. 8, 1763). In *Entick v. Carrington*, another case brought in trespass, Charles Pratt, Chief Justice of the Common Pleas (and, from July 1765, Lord Camden), rejected the potential for a general warrant to overcome the protections otherwise afforded to dwellings. John Entick's home had been "rifled; [and] his most valuable secrets [ ] taken out of his possession," *before* he had been convicted of any crime. (1765) 19 Howell's State Trials 1029, 1064 (C.P.). "This power so claimed by the secretary of state," Pratt observed, "is not supported by one single citation from any law book extant. It is claimed by no other magistrate in this kingdom but himself." *Id.*; *see also* Donohue, *Original*, *supra* note 15, at 1196–99 (discussing *Entick*). The reason for an absence of such authority was apparent: "The great end, for which men entered into society, was to secure their property." *Entick*, 19 Howell's State Trials, at 1066. The Chief Justice continued:

> By the laws of England, every invasion of private property, be it ever so minute, is a trespass. No man can set his foot upon my ground without my license, but he is liable to an action, though the damage be nothing; which is proved

Upon crossing the Atlantic, the American colonists expected the same protections that they held in England. When the Crown failed to respect the common law limits, the seeds of revolution were sown. In his celebrated oration in *Paxton's Case* in 1761, James Otis declared, "[O]ne of the most essential branches of English liberty is the freedom of one's house. A man's house is his castle; and whilst he is quiet, he is as well guarded as a prince in his castle."[18] The following year, John Dickinson, author of *Letters from a Farmer in Pennsylvania,* invoked the same ancient liberty. He attacked the Townshend Acts, which allowed the Crown to enter into "any HOUSE, warehouse, shop, cellar, or other place."[19] John Adams observed in 1774,

> An Englishmans dwelling House is his Castle. The Law had erected a Fortification round it—and as every Man is Party to the Law, i.e., the Law is a Covenant of every Member of society with every other Member, therefore every Member of Society has entered into a solemn Covenant with every other that he shall enjoy in his own dwelling House as compleat a security, safety and Peace and Tranquility as if it was surrounded with Walls of

---

by every declaration in trespass, where the defendant is called upon to answer for bruising the grass and even treading upon the soil.

Id. The sanctity of the home so permeated legal culture that the political elite spoke of it in Westminster. William Pitt (the Elder), 1st Earl of Chatham and Lord Privy Seal, declared:

> The poorest man may, in his cottage, bid defiance to all the forces of the Crown. It may be frail; its roof may shake; the wind may blow through it; the storm may enter; the rain may enter; but the King of England may not enter; all his force dares not cross the threshold of the ruined tenement.

THOMAS M. COOLEY, A TREATISE ON THE CONSTITUTIONAL LIMITATIONS WHICH REST UPON THE LEGISLATIVE POWER OF THE STATES OF THE AMERICAN UNION 425 n.1 (7th ed. 1903) (quoting Chatham). *See also* Donohue, *Original*, *supra* note 15, at 1238 (quoting and discussing Chatham's statement in Parliament).

18. Brief of James Otis, Paxton's Case (Mass. Sup. Ct. 24–26 Feb. 1761). *Cf.* Raleigh, Opinion, 3 MASSACHUSETTS SPY, Apr. 29, 1773, at 1, cols. 1–2 (discussing the problems with royal officers seizing traders' property without "proper cause"). *See also* Donohue, *Original*, *supra* note 15, at 1251.

19. John Dickinson, *Letter IX*, *in* EMPIRE AND NATION: LETTERS FROM A FARMER IN PENNSYLVANIA 51, 54 (Forrest McDonald ed., Liberty Fund Indianapolis 2d ed. 1999), http://oll.libertyfund.org/titles/690. For Dickinson, "[T]he greatest asserters of the rights of *Englishmen* have always strenuously contended, that *such a power* was dangerous to freedom, and expressly contrary to the common law, which ever regarded a man's *house* as his castle, or a place of perfect security." *Id.*; *see also* Donohue, *Original*, *supra* note 15, at 1261 (discussing Dickinson's letter).

> Brass, with Ramparts and Palisadoes and defended with a Garrison and Artillery.[20]

The Fourth Amendment cemented the home as a protected sphere into the U.S. Constitution.[21] It prohibited entry outside of limited circumstances absent a warrant supported by oath or affirmation relating to a named offense and particularly describing the place or persons to be searched and persons or things to be seized.[22]

The common law legacy persisted in American legal thought.[23] In 1833 Justice Joseph Story noted in his *Commentaries on the Constitution* that the Fourth Amendment amounted to "little more than the affirmance of a great constitutional doctrine of the common law."[24] Thirty-five years later Thomas Cooley wrote in his treatise: "The maxim that 'every man's house is his castle,' is made part of our constitutional law in the clauses prohibiting unreasonable searches and seizures, and has always been looked upon as of high value to the citizen."[25] In 1886, Justice Bradley recalled Chief Justice Pratt's judgment in *Entick*: "The principles laid down in this opinion affect the very essence of constitutional liberty and security."[26] Bradley continued:

> [T]hey apply to all invasions on the part of the government and its employees of the sanctity of a man's home and the privacies of life. It is not the breaking of his doors, and the rummaging of his drawers, that constitutes the essence of the offence; but it is the invasion of his indefeasible right of personal security, personal liberty, and private property.[27]

---

20. John Adams, *Adams' Minutes of the Review*, *in* 1 LEGAL PAPERS OF JOHN ADAMS 128, 137 (L. Kinvin Wroth & Hiller B. Zobel eds., 1965).

21. *See* Donohue, *Original*, *supra* note 15, at 1188.

22. *See id.* at 1193.

23. It also continued to be reflected in English law and legal treatises. *See, e.g.*, FRANCIS LIEBER, ON CIVIL LIBERTY AND SELF-GOVERNMENT 60 (Theodore D. Woolsey ed., J.B. Lippincott & Co. 3d ed. 1883) ("[N]o man's house can be forcibly opened, or he or his goods be carried away after it has thus been forced, except in cases of felony, and then the sheriff must be furnished with a warrant, and take great care lest he commit a trespass. This principle is jealously insisted upon.").

24. JOSEPH STORY, 3 COMMENTARIES ON THE CONSTITUTION OF THE UNITED STATES § 1895 (Boston, Hilliard, Gray & Co. 1833).

25. COOLEY, *supra* note 17, at 425–26; *see also* Donohue, *Original*, *supra* note 15, at 1307 (discussing Cooley's writings on the Fourth Amendment).

26. Boyd v. United States, 116 U.S. 616, 630 (1886); *see also* Donohue, *Original*, *supra* note 15, at 1308–13 (discussing the historical and legal background of *Boyd*).

27. *Boyd*, 116 U.S. at 630; *see also* Bram v. United States, 168 U.S. 532, 544 (1897) (commenting in relation to *Boyd*, "[I]t was in that case demonstrated that [the Fourth and Fifth Amendments] contemplated perpetuating, in their full effi-

To provide a remedy for a violation of the right, in 1914 the Court adopted the exclusionary rule, prohibiting the government from using evidence obtained from an unreasonable search or seizure.[28] The case, *Weeks v. United States*, arose from the arrest of a resident of Kansas City, Missouri.[29] While the suspect was being held in custody, law enforcement went to his home, found a hidden key, entered the house, and conducted a search.[30] The Court balked at the officers' actions, as well as those of a U.S. marshal, who similarly searched the home.[31] Neither search had been supported by a warrant.[32] Absent a remedy, the right could not be secured. The Court explained, "[T]he Fourth Amendment . . . put the courts of the United States and Federal officials, in the exercise of their power and authority, under limitations and restraints [and] . . . forever secure[d] the people, their persons, houses, papers and effects against all unreasonable searches and seizures under the guise of law."[33]

Whatever position one may have on the exclusionary rule as an effective, or even a constitutional, remedy, the fact that the Court considered it necessary underscored the distinction between the

---

cacy, by means of a constitutional provision, principles of humanity and civil liberty, which had been secured in the mother country only after years of struggle, so as to implant them in our institutions in the fullness of their integrity, free from the possibilities of future legislative change.").

28. Weeks v. United States, 232 U.S. 383, 398 (1914).

29. *Id.* at 387.

30. *Id.* at 386.

31. *Id.* at 386.

32. *Id.*

33. *Id.* at 391–92. A few years after *Weeks*, the Court considered a parallel fact pattern in *Silverthorne Lumber Co. v. United States*, 251 U.S. 385 (1920). Frederick Silverthorne had been indicted and arrested, and, while detained, a U.S. marshal had gone to his business and seized his books and papers. *Id.* at 390. Using the material already in its possession, the government had then drafted a new warrant to justify its actions. *Id.* at 391. The Court found that it was not permissible to allow the government to benefit from the illegal act. *Id.* at 391–92. Justice Holmes, writing for the Court, explained that allowing such actions would "reduce[ ] the Fourth Amendment to a form of words. The essence of a provision forbidding the acquisition of evidence in a certain way is that not merely evidence so acquired shall not be used before the Court but that it shall not be used at all." *Id.* at 392 (citations omitted). The Supreme Court did not apply the exclusionary rule to the states until 1961. Mapp. v. Ohio, 367 U.S. 643, 656–57 (1961). In 1995, the Court recognized a good faith exception to the exclusionary rule. Arizona v. Evans, 514 U.S. 1, 14 (1995). This includes when police employees err in maintaining a database. Herring v. United States, 555 U.S. 135, 137 (2009). The exclusionary rule similarly does not apply where law enforcement relies on binding appellate precedent or on statutes invalidated subsequent to the search. Davis v. United States, 564 U.S. 229, 232, 239 (2011).

protections afforded to the private sphere, marked by the home, and public space.[34]

For just as the home was sacred, what happened outside the home was rather less so.[35] A decade after *Weeks*, the Supreme Court

34. For a comprehensive article on the exclusionary rule, see generally Christopher Slobogin, *The Exclusionary Rule: Is It on Its Way Out? Should It Be?*, 10 OHIO ST. J. CRIM. L. 341 (2013). But note that over the past century, the rule has proven highly contentious both in its form and its implementation.

A number of scholars support the exclusionary rule. *See generally, e.g.*, Craig M. Bradley, *Reconceiving the Fourth Amendment and the Exclusionary Rule*, 73 LAW & CONTEMP. PROBS. 211 (2010); Thomas K. Clancy, *The Fourth Amendment's Exclusionary Rule as a Constitutional Right*, 10 OHIO ST. J. CRIM. L. 357 (2013); Lawrence Crocker, *Can the Exclusionary Rule Be Saved?*, 84 J. CRIM. L. & CRIMINOLOGY 310 (1993); Arthur G. LeFrancois, *On Exorcising the Exclusionary Demons: An Essay on Rhetoric, Principle, and the Exclusionary Rule*, 53 U. CIN. L. REV. 49 (1984); Timothy Lynch, *In Defense of the Exclusionary Rule*, 23 HARV. J. L. & PUB. POL'Y 711 (2000); Lawrence Rosenthal, *Seven Theses in Grudging Defense of the Exclusionary Rule*, 10 OHIO ST. J. CRIM L. 523 (2013); Scott E. Sundby, *Everyman's Exclusionary Rule: The Exclusionary Rule and the Rule of Law (or Why Conservatives Should Embrace the Exclusionary Rule)*, 10 OHIO ST. J. CRIM. L. 393 (2013); Lane V. Sunderland, *The Exclusionary Rule: A Requirement of Constitutional Principle*, 69 J. CRIM. L. & CRIMINOLOGY 141 (1978); Donald E. Wilkes, Jr., *A Critique of Two Arguments Against the Exclusionary Rule: The Historical Error and the Comparative Myth*, 32 WASH. & LEE L. REV. 881 (1975).

Other scholars have been sharply critical of the exclusionary rule or the so-called "good faith" exception to the rule. *See generally, e.g.*, Morgan Cloud, *Judicial Review and the Exclusionary Rule*, 26 PEPP. L. REV. 835 (1999) (criticizing the Supreme Court's focus on deterring police misconduct underlying good faith exception); David Gray, *A Spectacular Non Sequitur: The Supreme Court's Contemporary Fourth Amendment Exclusionary Rule Jurisprudence*, 50 AM. CRIM L. REV. 1 (2013); Kit Kinports, *Culpability, Deterrence, and the Exclusionary Rule*, 21 WM. & MARY BILL RTS. J. 821 (2013) (criticizing the Supreme Court's focus on deterring police misconduct underlying good faith exception); Wayne R. LaFave, *The Smell of* Herring: *A Critique of the Supreme Court's Latest Assault on the Exclusionary Rule*, 99 J. CRIM. L. & CRIMINOLOGY 757 (2009) (criticizing a recent "good faith" decision); Eugene Milhizer, *The Exclusionary Rule Lottery*, 39 U. TOL. L. REV. 755 (2008); Eugene Milhizer, *The Exclusionary Rule Lottery Revisited*, 59 CATH. U. L. REV. 747 (2010); Eugene R. Milhizer, *Debunking Five Great Myths About the Fourth Amendment Exclusionary Rule*, 211 MIL. L. REV. 211 (2012); Richard E. Myers II, *Fourth Amendment Small Claims Court*, 10 OHIO ST. J. CRIM. L. 571 (2013); Gregory D. Totten, Peter D. Kossoris, & Ebbe B. Ebbesen, *The Exclusionary Rule: Fix It, but Fix It Right*, 26 PEPP. L. REV. 887 (1999); Silas Wasserstrom & William J. Mertens, *The Exclusionary Rule on the Scaffold: But Was It a Fair Trial?*, 22 AM. CRIM. L. REV. 85 (1984) (criticizing the good faith exception); Michael T. Kafka, *The Exclusionary Rule: An Alternative Perspective*, Note, 27 WM. MITCHELL L. REV. 1895 (2001).

35. Orin Kerr, in his postulation of the equilibrium theory of the Fourth Amendment, lists as his first rule of the status quo in rule zero: "[T]he police are always free to watch suspects in public. They can walk up to suspects and monitor them at close range and ask them questions." Orin S. Kerr, *An Equilibrium-Adjustment Theory of the Fourth Amendment*, 125 HARV. L. REV. 476, 484 (2011) (footnote

declared in *Hester v. United States* that the Fourth Amendment protection of "persons, houses, papers and effects" did not extend to "open fields."[36] Citing Blackstone's *Commentaries*, Justice Holmes added, "The distinction between the latter and the house is as old as the common law."[37] While the home held a special place in the law, what happened outside of it obtained fewer protections.

As the administrative state expanded, whenever the Court confronted potential exceptions, such as those that arose with regard to health inspections, the bench was closely divided.[38] It was only when the medical concern was sufficiently acute, and the purpose and object of the inspection sufficiently targeted, that such intrusions could be tolerated. A suspected infestation of rats would suffice; general inspection of the home's structure would not.[39] Outside of any emergency situation, the unwarranted search of a

---

omitted). He takes it as given that police "can walk the beat and observe whatever they see in public." *Id.* The reason that this could even be considered a given stems from the common law protections of the home.

36. Hester v. United States, 265 U.S. 57, 59 (1924). The case evolved in the shadow of the Eighteenth Amendment. U.S. CONST. amend. XVIII, *repealed by* U.S. CONST. amend. XXI. Revenue officers, hiding outside Hester's home, saw him give a bottle of what appeared to be moonshine to another person. 265 U.S. at 58.

37. *Hester*, 265 U.S. at 59 (citing 4 WILLIAM BLACKSTONE, COMMENTARIES *223, *225–*26).

38. *See, e.g.*, Frank v. Maryland, 359 U.S. 360 (1959) (upholding over four dissenters a Baltimore City health inspector's search for the source of a rat infestation without a warrant). In *Ohio ex rel. Eaton v. Price*, 364 U.S. 263 (1960), the Court split evenly, leaving in place the decision of the Ohio Supreme Court upholding a housing inspector's decision to enter a plumber's residence without a warrant. The opinion, split four to four, is without force of precedent. But in this case, the four Justices that did not join the opinion in *Ohio* had already publicly expressed their opinion that *Frank* controlled, *id.* at 264, leading the other four Justices to write an opinion declaring *Frank* "the dubious pronouncement of a gravely divided Court" and calling for reversal, *id.* at 269.

39. In the 1967 case *Camara v. Mun. Court*, the Court stated that the purpose of the Fourth Amendment, enforceable against the states through the Fourteenth Amendment, was to protect citizens against "unreasonable searches and seizures." 387 U.S. 523, 528 (1967). Outside of carefully defined contours, an unconsented, warrantless search is *per se* unreasonable. *Id.* at 528–29. In *Camara*, the appellant had refused to allow housing inspectors access to his property in order to determine whether he was in violation of the occupancy permit. *Id.* at 525. Delivering the opinion of the Court, Justice White distinguished the case from *Frank v. Maryland*, in which the intrusion "touch[ed] at most on the periphery" of the Fourth Amendment given the importance of the municipal fire, health, and housing inspection programs designed to ensure the habitability of the structure. *Id.* at 530 (citing *Frank*, 359 U.S. at 367). In *Camara*, a general inspection was too attenuated a connection to necessity to warrant overriding the protections otherwise extended to the home. *Id.* at 533. White noted that warrantless powers of entry could be used for great mischief. Quoting *Johnson v. United States*, 333 U.S. 10, 14 (1948)

private home was per se unreasonable under the Fourth Amendment.

B. Papers

At the founding, papers in the home were subject to protections similar to those afforded to other items (and activities) within the dwelling house.[40] Government officials could not simply cross the threshold at will to read or to seize them. Beyond this, consistent with common law, *judges did not have the authority to issue search warrants to seize papers as evidence of criminal activity*.[41] This point is worth emphasizing in the contemporary environment, not least because the Director of the Federal Bureau of Investigation, in the context of the encryption debate, has taken to repeating a falsehood: that, with the appropriate process, the government has always had access to what people think, say, and write.[42] It has not. For nearly two hundred years, the government could *not* obtain private papers—even with a warrant—when they were to be used as evidence of criminal activity.

(finding officers' warrantless entry into a hotel room from which the odor of burning opium emanated unconstitutional), he wrote,

> The right of officers to thrust themselves into a home is also a grave concern, not only to the individual but to a society which chooses to dwell in reasonable security and freedom from surveillance. When the right of privacy must reasonably yield to the right of search is, as a rule, to be decided by a judicial officer, not by a policeman or government enforcement agent. *Camara*, 387 U.S. at 529.

40. The history of this protection duplicates that which is detailed in Part II(A), *supra*. For further discussion of the special place afforded to papers, see generally Donohue, *Original*, *supra* note 15.

41. See Donohue, *Original*, *supra* note 15, at 1308–14 and *infra* for discussion of the mere evidence rule and its roots in common law.

42. *See, e.g.*, James B. Comey, Dir., Fed. Bureau of Investigation, Expectations of Privacy: Balancing Liberty, Security, and Public Safety, Remarks to the Center for the Study of American Democracy Biennial Conference at Kenyon College, at 2–3 (Apr. 6, 2016) (transcript available at https://www.fbi.gov/news/speeches/expectations-of-privacy-balancing-liberty-security-and-public-safety); James B. Comey, Dir., Fed. Bureau of Investigation, Remarks to the Am. Bar Ass'n Annual Meeting, Finding the Balance We Need in Law and Life, at 2 (Aug. 5, 2016) (transcript available at https://www.fbi.gov/news/speeches/finding-the-balance-we-need-in-law-and-life); *The Encryption Tightrope: Balancing Americans' Security and Privacy: Hearing Before the H. Comm. on the Judiciary*, 114th Cong. 52–53 (2016) (statement of James B. Comey, Dir., Fed. Bureau of Investigation) ("[F]rom the founding of this country, it was contemplated that law enforcement could go into your house with appropriate predication and oversight. So, to me, the logic of that tells me they wouldn't have imagined any box or storage area or device that could never be entered.").

In the nineteenth century, the Court extended the protection of documents to papers traveling through the post. In the 1878 case *Ex parte Jackson*, the Court considered whether a lottery circular, sent in a closed envelope, deserved Fourth Amendment protections.[43] Justice Field, writing for the Court, noted that Congress's authority "to establish post offices and post roads" extended beyond merely designating the appropriate routes, to include carriage of the mail, its safe and swift transit, and its prompt delivery.[44] But while the right to carry the mail might mean that Congress could determine what could be carried *en route*, it did not give Congress the ability to *open* materials in transit.[45] To read the Constitution in such a manner would give Congress the authority to override rights retained by the people.

"Letters and sealed packages . . . in the mail," Field wrote, "are as fully guarded from examination and inspection, except as to their outward form and weight, *as if they were retained by the parties forwarding them in their own domiciles*."[46] He underscored the importance of the text: "The constitutional guaranty of the right of the people to be secure in their papers against unreasonable searches and seizures extends to their papers, thus closed against inspection, wherever they may be."[47] Field explained,

> Whilst in the mail, they can only be opened and examined under like warrant, issued upon similar oath or affirmation, particularly describing the thing to be seized, as is required when papers are subjected to search in one's own household. No law of Congress can place in the hands of officials connected with the postal service any authority to invade the secrecy of letters and such sealed packages in the mail; and all regulations adopted as to mail matter of this kind must be in subordination to the great principle embodied in the fourth amendment of the Constitution.[48]

Field recognized the close relationship between the interests protected by the Fourth Amendment and those protected by the First Amendment.[49] Any restrictions on the transfer of mail also violated the freedom of the press: "[l]iberty of circulating," Field pointed out, "is as essential to that freedom as liberty of publish-

43. *Ex parte* Jackson, 96 U.S. 727, 728, 733 (1877).
44. *Id.* at 732.
45. *Id.* at 733.
46. *Id.* (emphasis added).
47. *Id.*
48. *Id.*
49. *Ex parte Jackson*, 96 U.S. at 733.

ing."[50] It meant nothing to claim that the press was free if Congress could then interfere with delivery of the newspapers, or pass laws limiting the circulation of written material.[51]

Even as the Court allowed for private correspondence to be subject to the same protections as papers held within the home, a terrestrial test applied: documents became protected *as if they still resided* inside one's domicile. Delivering the letter did not divorce it of the protections it otherwise enjoyed. In a three-dimensional world, where the government itself carried the letter, a clear line could be drawn. Absent good cause, officials could neither break into a study nor tear open an envelope *en route* to gain access.

Ex parte Jackson dealt with a lottery circular sent through the post. Other efforts to flesh out the contours of protections applied to papers followed. Just three years prior to the Court's ruling in *Jackson*, Congress had passed a statute to prevent smuggling.[52] The law authorized judges to direct the production of private books, invoices, and papers in revenue cases.[53] Fourteen years later, in *Boyd v. United States*, the Supreme Court declared the provision to be unconstitutional and void.[54] In doing so, the Court recognized the close relationship between the Fourth and Fifth amendments, noting that:

> [A] compulsory production of a man's private papers to establish a criminal charge against him, or to forfeit his property, is within the scope of the Fourth Amendment to the Constitution in all cases in which a search and seizure would be, because it is a material ingredient, and effects the sole object and purpose of search and seizure.[55]

The Court dismissed Congress's effort to gain control over private papers as being almost arrogant, noting the absence of any similar effort in history, despite the egregious nature of measures implemented by the British government. "Even the act under which the obnoxious writs of assistance were issued," the Court wrote, "did not go as far as this."[56] The effort to recover stolen goods, moreover, for which a warrant historically *had* been required, fell short of

50. *Id.*

51. *Id.* at 734.

52. Act of June 22, 1874, ch. 391, 18 Stat. 186.

53. Sec. 5, 18 Stat. at 187 (requiring surrender of books, invoices, and papers required in civil suits under revenue laws).

54. Boyd v. United States, 116 U.S. 616, 638 (1886).

55. *Id.* at 622.

56. *Id.* at 623.

the level of intrusion now contemplated by the legislature.[57] The Court explained:

> The search for and seizure of stolen or forfeited goods . . . are totally different things from a search for and seizure of a man's private books and papers for the purpose of obtaining information therein contained, or of using them as evidence against him. The two things differ *toto coelo*. In the one case, the government is entitled to the possession of the property; in the other it is not.[58]

Justice Bradley, writing for the Court in *Boyd*, cited back to Coke and noted Otis's oration in *Paxton's Case*.[59] The government could not break into an individual's home to obtain the documents; neither could it force an individual to produce the same information, as such an action would trigger the protection against self-incrimination.[60]

Boyd evolved into the "mere evidence" rule, which established that only criminal instrumentalities and stolen goods could be recovered by warrants consistent with the Fourth Amendment.[61] In 1917, when Congress introduced the first law giving federal law enforcement the formal authority to issue search warrants, the legislature was careful to hew to the doctrinal line.[62] It limited warrants for search and seizure to property "stolen or embezzled in violation of a law of the United States," "used as the means of committing a felony," or used to aid a foreign government in violating "any penal statute[,] . . . treaty or the law of nations".[63] These reflected the rule that only the fruits or instrumentalities of crime could be obtained via warrant.

---

57. Donohue, *Original*, *supra* note 15.

58. *Boyd, supra* note 54, at 623.

59. *Id.* at 625, 629 (quoting *Paxton's Case*). *See also supra* Part II(A).

60. *See Boyd*, 116 U.S. at 630–35.

61. *See* Donohue, *Original*, *supra* note 15, at 1308–14 (discussing *Boyd* and the origins of the mere evidence rule, and suggesting that instead of inventing it out of whole cloth, the Court's adherence to it reflected a long practice of rejecting the use of search and seizure to obtain evidence against individuals.).

62. Act of June 15, 1917, ch. 30, tit. XI, § 2, 40 Stat. 217, 228; William T. Rintala, *The Mere Evidence Rule: Limitations on Seizure Under the Fourth Amendment*, 54 CAL. L. REV. 2099, 2103 (1966) (recognizing the statute as "the first general statute authorizing the issuance of search warrants to federal officers"); *see generally* Thomas H. Davis, *The "Mere Evidence" Rule in Search and Seizure*, 35 Mil. L. Rev. 101 (1967) (analyzing the history and legal background of the mere evidence rule).

63. § 2, 40 Stat. at 228, 230.

In 1921, the mere evidence rule reached what one commentator has referred to as its "zenith."[64] In *Gouled v. United States* the Court considered whether the warrantless removal of a paper from a defendant's office violated the Fourth Amendment.[65] Justice Clarke, on behalf of the Court, observed that making a search by stealth did not make it *more* reasonable than if the same were accomplished "by force or illegal coercion."[66] He continued,

> The security and privacy of the home or office and of the papers of the owner would be as much invaded and the search and seizure would be as much against his will in the one case as in the other, and it must therefore be regarded as equally in violation of his constitutional rights.[67]

Based on *Boyd*, the admission of the papers as evidence violated the Fifth Amendment.[68]

The difficulty of differentiating the instrumentalities of crime from mere evidence ultimately led to the demise of the mere evidence rule.[69] But even as it fell from use, courts agonized over the implications of giving the government access to private papers.[70] According to one commentator, the reasons for this appear to be twofold.[71]

First was the risk that the government would engage in searches beyond what was required.[72] As Judge Learned Hand explained in 1926, "It is seldom that one finds a document containing evidence of crime which was not at one time used in its commission."[73] But to find such evidence often required "a thorough

64. Rintala, *supra* note 62, at 2105–13 (analyzing, *inter alia,* Marron v. United States, 275 U.S. 192 (1927); United States v. Lefkowitz, 285 U.S. 452 (1932); Foley v. United States, 64 F.2d 1 (5th Cir.), *cert. denied*, 289 U.S. 762 (1933)).

65. 255 U.S. 298, 303 (1921).

66. *Id.* at 305.

67. *Id.* at 305–06.

68. *Id.* at 306.

69. *See* Warden v. Hayden, 387 U.S. 294, 310 (1967). *Warden* was decided on May 29, 1967; in October of the same year, the Court heard oral argument in *Katz*, issuing its opinion that December. Katz v. United States, 389 U.S. 347 (1967). Notably, in *Warden*, the circumstances of the search under consideration, which involved a fleeing felon, *Warden*, 387 U.S. at 297–98, overlapped with a long-standing exception to the warrant requirement, making the question of the mere evidence rule rather beside the point, *see* Donohue, *Original*, *supra* note 15, at 1228–35 (discussing the history of the fleeing felon exception).

70. *See* Rintala, *supra* note 62, at 2115.

71. *Id.*

72. *Id.*

73. United States v. Kirschenblatt, 16 F.2d 202, 204 (2d Cir. 1926); *see also* Rintala, *supra* note 62, at 2115 (citing and discussing *Kirschenblatt*).

search of all that the offender has."[74] Should the courts allow this, however, they would be endorsing "exactly what [the Fourth Amendment] was designed to prevent."[75] "Therefore," Hand continued, "we cannot agree that the power extends beyond those which are a part of the forbidden act itself."[76]

Second, private papers can reveal the most intimate details of an individual's life. As William Rintala observed,

> Private papers, be they diary or political tract, are felt to stand on a different footing from other kinds of personal property. This difference can be attributed at least in part to the fact that they are products of the mind; to invade this realm is to strip the individual of the last vestige of privacy.[77]

C. Voice Communications

As new technologies extended interpersonal communications beyond dwellings and channels of written correspondence, novel questions regarding the extent of Fourth Amendment protections emerged.[78] Initially, the Court came down on the side of the traditional distinction between private and public space, drawing the line at the walls of the home.[79] Trespass impinged upon individual

74. *Kirschenblatt*, 16 F.2d at 204.

75. *Id.*; *see also* Rintala, *supra* note 62, at 2115.

76. *Kirschenblatt*, 16 F.2d at 204.

77. Rintala, *supra* note 62, at 2115–16 (footnote omitted).

78. For an interesting discussion of telegraphy and why it did not give rise to similar issues, see Susan W. Brenner, *The Fourth Amendment in an Era of Ubiquitous Technology*, 75 MISS. L. J. 1, 12–16 (2005). For detail on the evolution of the telephone and its place in communications, see *id.* at 17–21.

79. I depart here from the account offered by Professor Thomas Clancy in his excellent treatise on the Fourth Amendment. In that work, he suggests that "[b]eginning with *Olmstead v. United States*, the Court limited Fourth Amendment rights in two important ways. First, the only things protected were tangible objects, such as houses, papers, and physical possessions. Second, those objects were only protected against physical invasions." THOMAS K. CLANCY, THE FOURTH AMENDMENT: ITS HISTORY AND INTERPRETATION § 3.2.2 (2d ed. 2014) (footnote omitted) (describing Olmstead v. United States, 277 U.S. 438 (1928)). Reflecting its common law origins, the Fourth Amendment had always been treated in this manner, suggesting that Fourth Amendment rights were not narrowed or newly-limited, but merely continued. *Olmstead* continued the traditional interpretation, until the Court eventually moved to recognize that the same privacy interests in the traditional purview of the Fourth Amendment were implicated by voice communication technologies. *See generally* Silverman v. United States, 365 U.S. 505 (1961) (finding eavesdropping with a listening device by means of unauthorized physical penetration a violation of the Fourth Amendment). The "property-based theories of *Boyd* and *Olmstead*," as Clancy characterizes the concept, *supra*, at § 3.2.3, actually extended beyond these cases to the founding generation's initial understanding of

privacy. Conversely, the absence of physical entry meant that no privacy interest had been disturbed.

In *Olmstead v. United States*, the first case dealing with new communications technology, the Supreme Court held that the wiretapping of an individual's private telephone line did not fall within constitutional protections, as the government had not engaged in a physical trespass.[80] Chief Justice Taft, delivering the opinion of the Court, wrote, "[U]nless there has been an official search and seizure of his person, or such a seizure of his papers or his tangible material effects, or an actual physical invasion of his house '*or curtilage*' for the purpose of making a seizure," neither wiretapping nor electronic eavesdropping absent a warrant violated an individual's Fourth Amendment rights.[81]

A few observations about Taft's language deserve note. First, this is the first time that the Supreme Court used the word "curtilage" in relation to the validity of a search under the Fourth Amendment.[82] State courts, in contrast, for more than a century had considered the validity of search and seizure under state constitutional law to turn on whether the action took place within the curtilage.[83]

---

the Fourth Amendment. *See* Donohue, *Original*, *supra* note 15, at 1192–93 (arguing that the original meaning of the Fourth Amendment limited general searches and seizures and required specific warrants, and emphasizing the importance of the common law in interpreting reasonableness). Numerous secondary sources discuss *Olmstead*, *Goldman*, and *Silverman* as precursors to *Katz*. *See, e.g.,* Weaver, *supra* note 12, at 1150.

80. *Olmstead*, 277 U.S. at 466.

81. *Id.* (emphasis added).

82. Search using Westlaw's All Federal and All State Cases database *(curtilage OR curtelage OR curtailage) AND (seizure or warrant or warrantless)* 1750 to 1921; Search using Lexis Advance in the All Federal Cases and State Cases database with exact phrase "curtilage" and any of these terms "search or seizure or warrant or warrantless" 1750 to 1921; *Id.*, using exact phrases curtilage, curtelege, and curtailage.

83. *See, e.g.*, Commonwealth v. Intoxicating Liquors, 110 Mass. 182, 186 (1872) (considering whether the outbuildings contained within the curtilage were covered by a warrant); Pond v. People, 8 Mich. 150, 181 (1860) (finding in the context of the search and seizure of a person that a fence is not necessary for a net house to be considered within the curtilage if the space is no larger than that which is usually occupied for the purposes of dwelling and outbuildings); Haggerty & Nobles v. Wilber & Barnet, 16 Johns. 287, 288 (N.Y. Sup. Ct. 1819) (holding that a sheriff has the authority to break open and seize goods, but if they are located within the curtilage, the sheriff is precluded from entering unless the outer door is open); Douglass v. State, 14 Tenn. 525, 529 (1834) (the validity of seizure and arrest of rioters located in a smoke-house depends upon whether the building is considered within the curtilage); Parrish v. Commonwealth, 81 Va. 1, 4 (1884) (requiring a warrant for the search of corn in a tobacco house within the curti-

Second, Taft borrowed the term from criminal law, where it derived from the common law of burglary, which increased criminal penalties for illegal activity within the curtilage.[84] Disagreement marked what, precisely, counted as the curtilage.[85] In the early 19th century, for instance, *Jacob's Law Dictionary* defined it as "[a] court-yard, back-side, or piece of ground lying near and belonging to a dwelling-house."[86] It incorporated buildings like out houses and store-houses occasionally used for sleeping.[87] The way in which Taft

---

lage), *overruled in part on other grounds by* Fortune v. Commonwealth, 112 S.E. 861, 867 (Va. 1922); Pettus v. Commonwealth, 96 S.E. 161, 162–63 (Va. 1918) (search of a room over a grocery store not considered within the curtilage).

84. Four years prior to *Olmstead*, Justice Holmes had cited back to Blackstone's *Commentaries* and the common law of burglary in support of establishing the open fields doctrine. Hester v. United States, 265 U.S. 57, 59 (1924) (citing 4 WILLIAM BLACKSTONE, COMMENTARIES *225) ("For no distant barn, warehouse, or the like, are under the same privileges, nor looked upon as a man's castle of defence: nor is a breaking open of houses wherein no man resides, and which therefore for the time being are not mansion-houses, attended with the same circumstances of midnight terror."). Later cases attributed Taft's reference to curtilage to stem from the common law of burglary. *E.g.* United States v. Dunn, 480 U.S. 294, 300 (1987).

85. State v. Langford, 12 N.C. 253, 254 (1827) ("[W]riters do not precisely agree as to what constitutes the curtilage."); People v. Taylor, 2 Mich. 250, 252 (1851) ("The definitions of [curtilage in] Bouviere and Chitty do not strictly agree with [other law dictionaries].").

86. *Curtilage*, 2 JACOB'S LAW DICTIONARY 171 (New York, Riley 1811); *see also* State v. Twitty, 2 N.C. 102, 102 (1794) (defining it as "a piece of ground either inclosed or not, that is commonly used with the dwelling house."); State v. Shaw, 31 Me. 523, 527 (1850) ("The curtilage of a dwellinghouse is a space, necessary and convenient and habitually used, for the family purposes, the carrying on of domestic employments. It includes the garden, if there be one.").

87. *See, e.g.*, State v. Brooks, 4 Conn. 446, 448–49 (1823) ("The mansion not only includes the dwelling-house, but also the out-houses, such as barns, stables, cow-houses, dairy-houses and the like, if they be parcel of the messuage, though they be not under the same roof or joining continuous to it.") (internal quotation marks omitted) (considering a barn to be an out-house and thus protected under statutory provisions); People v. Parker, 4 Johns 424, 424 (N.Y. Sup. Ct. 1809) (placing store house specifically not used for sleeping, and not enclosed with the house, outside the curtilage); State v. Wilson, 2 N.C. 242, 242 (1795) ("All out houses standing in the same yard with the dwelling-house, and used by the owner of the dwelling-house as appurtenant thereto, whether the yard be open or enclosed, are in the eye of the law parts of the dwelling-house; and will satisfy that word used in an indictment of burglary.") (placing storehouses used occasionally for sleeping within the curtilage); Gage v. Shelton, 3 Rich 242, 249–50 (S.C. App. L. & Eq. 1832) (noting that any out house contributory to the mansion, if placed close enough that burning it would put the dwelling in danger, was protected against arson); Douglass v. State, 14 Tenn. 525, 529–30 (1834) (finding a smokehouse to be within the curtilage of the mansion house); *see also Twitty*, 2 N.C. at 103 (considering the out house to be within the curtilage of the home); *cf. Langford*, 12 N.C.

used the term in *Olmstead*, though, allowed for a later reading that considered the curtilage coterminous with the home itself. The Court's holding in *Hester*, the year before *Olmstead*, which distinguished between open fields and the home, reinforced this reading.[88]

Third, beyond sowing the seeds for a narrower protected sphere, Taft gave the mistaken impression that the term carried weight in the Court's Fourth Amendment jurisprudence. In support of his framing, he quoted the 1921 case of *Amos v. United States*, which dealt with a violation of revenue laws.[89] In *Amos*, law enforcement had arrived at the defendant's home and asked his wife for entry.[90] Performing a warrantless search, they found a bottle of illicitly distilled whisky in a barrel of peas.[91] After the jury was sworn in, but before evidence had been presented, the defendant in the criminal case presented a sworn petition to the court, requesting that his private property be returned to him.[92] According to the *Amos* Court, the petition stated that the whiskey had been seized by "officers of the Government in a search of defendant's house and store '*within his curtilage*,' made unlawfully and without warrant of any kind, in violation of his rights under the Fourth and Fifth Amendments to the Constitution of the United States."[93] The lan-

---

at 254 (tying the extent of the curtilage to the span of the dwelling house "and such houses as are used as part or parcel thereof"); Commonwealth v. Sanders, 32 Va. 751, 753 (Va. Gen. Ct. 1835) (storehouse not within the curtilage of a tavern). The term was also used in other areas of the law, further obscuring the meaning. In cases involving land lotteries and ownership, for instance, it included yards and other parcels of land convenient to indwellers. Southall v. M'Keand, Wythe 95, 102, 1794 WL 327, at *5 (Va. High Ch. Nov. 6, 1794). Private actions involving matters within the curtilage of others' homes were restricted. *See, e.g.*, Morgan v. Banta, 4 Ky. (1 Bibb) 579, 580 (1809); Coleman v. Moody, 14 Va. (1 Hen. & M.) 1, 2 (1809); Home v. Richards, 8 Va. (4 Call) 441, 441–42 (Va. Ct. App. 1798) ([both] cases dealing with writ of *ad quod damnum* in mill-dam situations). In Virginia, statutes restricted public takings of private property within the curtilage. Commonwealth v. Beeson, 30 Va. (3 Leigh) 821, 826 (Va. Gen. Ct. 1832) (noting that the statute imposed as a limit on the right of public takings "that in no case, without the consent of the owner, shall the mansion house, curtilage &c. [sic] be invaded for public purposes, whether with or without compensation."). Liens also turned on the concept of what fell within the curtilage. *See* Derrickson v. Edwards, 29 N.J.L. 468, 474 (N.J. 1861).

88. *Hester*, 265 U.S. at 59.

89. *Olmstead*, 277 U.S. at 461 (citing Amos v. United States, 255 U.S. 313, 315 (1921).).

90. *Amos*, 255 U.S. at 315.

91. *Id.* at 314–15.

92. *Id.* at 314.

93. *Id.*

guage of the criminal defendant's petition to the lower court was the only reference in *Amos* to the curtilage of the home.[94]

In *Olmstead*, Taft picked up on the language *in the criminal defendant's petition*, quoting it directly and then misquoting it later in the opinion as an alternative to, or potentially a synonym for, the home ("'or curtilage'").[95] Taft went on to rely on the absence of any *physical penetration* of the curtilage as grounds to consider wiretapping outside the contours of the Fourth Amendment.[96]

Justice Brandeis, joined by Justice Stone, presented a forceful dissent that objected to the emphasis on physical penetration, pointing to the interests at stake.[97] He argued that the interception of the conversation constituted an "unjustifiable intrusion . . . upon the privacy of the individual," and thus violated the Fourth Amendment.[98] Brandeis underscored what the "makers of our Constitution" had tried to accomplish: "They sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations."[99] He continued, "They conferred, as against the Government, the right to be let alone—the most comprehensive of rights and the right most valued by civilized men."[100] Brandeis warned that the Court had to look not just at the current context, but also what was coming down the pike. He cautioned,

> The progress of science in furnishing the Government with means of espionage is not likely to stop with wire-tapping. Ways 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.[101]

Brandeis was ahead of his time in identifying the privacy interests involved. The Court had yet to appreciate how technology had altered the impact of the traditional distinction between private

94. *See generally id.* The Court ruled for the defendant, saying that *Gouled*, and the mere evidence rule, controlled. *Id.* at 316.

95. Olmstead v. United States, 277 U.S. 438, 466 (1928).

96. *Id.*

97. *See generally id.* at 471 (Brandeis, J., dissenting); *Id.* at 488 (Stone, J., dissenting).

98. *Id.* at 478 (Brandeis, J., dissenting).

99. *Id.*

100. *Id.*

101. *Olmstead*, 277 U.S. at 474 (Brandeis, J., dissenting); *see also* Weems v. United States, 217 U.S. 349, 373 (1910) ("In the application of a constitution, therefore, our contemplation cannot be only what has been but of what may be. . . . Rights declared in words might be lost in reality. And this has been recognized.").

space and the public domain. A series of cases began hammering on the door.

In 1942, the Court considered federal agents' access to the office of an individual suspected of conspiring to violate criminal provisions of the Bankruptcy Act.[102] Agents went into an adjoining office, where they placed a listening device in a small aperture in the wall.[103] When the device failed, officers used a detectaphone to listen to conversations next door, which they recorded and transcribed using a stenographer.[104] Consistent with *Olmstead*, the Court found in *Goldman v. United States* that use of the detectaphone did not run afoul of the Fourth Amendment.[105]

In his dissent, Justice Murphy blasted the Court for not taking account of new technologies.[106] Referencing the acclaimed 1890 *Harvard Law Review* article written by Louis Brandeis and Samuel Warren, Murphy argued for a broader reading of the Fourth Amendment to protect individuals "against unwarranted intrusions by others" into their private affairs.[107] Although the language of the Fourth Amendment intimated protection against physical trespass, Murphy averred, "[I]t has not been the rule or practice of this Court to permit the scope and operation of broad principles ordained by the Constitution to be restricted, by a literal reading of its provisions, to those evils and phenomena that were contemporary with its framing."[108] Of greater importance were the privacy interests that the amendment was meant to protect.

Like Brandeis in *Olmstead*, Murphy recognized that the "conditions of modern life have greatly expanded the range and character of those activities which require protection from intrusive action by Government officials if men and women are to enjoy the full benefit of that privacy which the Fourth Amendment was intended to provide."[109] It was therefore the Supreme Court's "duty to see that this historic provision receives a construction sufficiently liberal and elastic to make it serve the needs and manners of each succeeding generation."[110] Murphy gave little countenance to whether or not a physical entry had occurred since "science has brought forth far

102. Goldman v. United States, 316 U.S. 129, 130–31 (1942).
103. *Id.* at 131.
104. *Id.* at 131–32.
105. *Id.* at 135.
106. *Id.* at 139 (Murphy, J., dissenting).
107. *Id.* at 136 (Murphy, J., dissenting) (citing Louis Brandeis & Samuel Warren, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890)).
108. *Goldman*, 316 U.S. at 138 (Murphy, J., dissenting).
109. *Id.*
110. *Id.*

more effective devices for the invasion of a person's privacy than the direct and obvious methods of oppression which were detested by our forebears and which inspired the Fourth Amendment."[111] To the extent that electronic surveillance made it possible to do what had hitherto been considered within the ambit of the Fourth Amendment, so, too, ought new technologies to be considered within the reach of the Constitution.

By the time *Silverman v. United States* was decided in 1961, the intrusiveness of new technologies on interests previously guarded by the walls of the home had become apparent.[112] The petitioner's brief in *Silverman* underscored the impact of recent advances, drawing attention to parabolic microphones "which can pick up a conversation three hundred yards away," experimental sound wave technology "whereby a room is flooded with a certain type of sonic wave . . . mak[ing] it possible to overhear everything said in a room without ever entering it or even going near it," and devices that could "pick up a conversation through an open office window on the opposite side of a busy street."[113] But the physical characteristics of a spike mike allowed the Court to distinguish the facts from *Olmstead*: in *Silverman*, since law enforcement had made physical contact with a heating duct, "an unauthorized physical penetration into the premises occupied by the petitioners" had occurred.[114]

In reaching its decision, the Court recognized the extent to which emerging technologies had proven contentious: "Eavesdropping accomplished by means of such a physical intrusion is beyond the pale of even those decisions in which a closely divided Court has held that eavesdropping accomplished by other electronic means did not amount to an invasion of Fourth Amendment rights."[115] At the same time, the Court doubled down on the importance of the home.[116] Trespass ruled the day.[117] The importance of

111. *Id.* at 139.

112. *See* Silverman v. United States, 365 U.S. 505, 508–09 (1961) (discussing petitioner's description of technology enabling recording of distant conversations).

113. *Id.* at 508–09 (internal quotation marks omitted); *see also* Weaver, *supra* note 12, at 1148 (discussing *Silverman*).

114. *Id.* at 509.

115. *Id.* at 509–10.

116. *Id.* at 511 ("The Fourth Amendment, and the personal rights which it secures, have a long history. At the very core stands the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion.").

117. The parallels between *Silverman* and *United States v. Jones*, 132 S. Ct. 945, 954 (2012), also decided on grounds of trespass, are of note, as *Jones* also signaled a growing concern for how new technologies may affect rights otherwise protected

drawing a distinction between the private and public realms underlay the Court's approach. Behavior in the former realm was protected. But in public, individuals assumed the risk that what they said and did would be witnessed, and potentially recalled, by others.

Silverman proved pivotal, foreshadowing the coming confrontation between new technologies and the protections guaranteed in the Fourth Amendment. While hewing to the traditional trespass doctrine, it noted the potential for "frightening paraphernalia which the vaunted marvels of an electronic age may visit upon human society."[118]

In summary, the Court's initial take when confronted by technology had been to construe the Fourth Amendment "in the light of what was deemed an unreasonable search and seizure when it was adopted."[119] As Taft explained in *Olmstead*, "Congress may of course protect the secrecy of telephone messages by making them, when intercepted, inadmissible in evidence. . . . But the courts may not adopt such a policy by attributing an enlarged and unusual meaning to the Fourth Amendment."[120] Where the public realm ended and private life began, a higher standard applied. Accordingly, in its June 1967 *Camara v. Municipal Court* decision, the Court came out strongly on the side of drawing a border at the walls of the home.[121] But the tension between new technologies and the existing doctrine had reached a boiling point. Just four months later, the Court in *Katz v. United States* extended the protection of the Fourth Amendment beyond physical property to include areas that individuals *considered* private.[122] In doing so, the Court raised new questions as to whether the shift to protect "people," not "places,"

---

under the Fourth Amendment, but relied on traditional trespass theory for its holding. *See* discussion *infra* Part III(D).

118. *Silverman*, 365 U.S. at 509; *see also* Alderman v. United States, 394 U.S. 165, 177–78 (1969); Berger v. New York, 388 U.S. 41, 45–47 (1967).

119. Olmstead v. United States, 277 U.S. 438, 465 (1928) (quoting Carroll v. United States, 267 U.S. 132, 149 (1925)). In *Olmstead*, Chief Justice Taft wrote on behalf of the Court, "The well known historical purpose of the Fourth Amendment . . . was to prevent the use of governmental force to search a man's house, his person, his papers and his effects; and to prevent their seizure against his will." *Id.* at 463. It was the home itself that was a constitutionally protected area. "The language of the Amendment," Taft suggested, "can not be extended and expanded to include telephone wires reaching to the whole world from the defendant's house or office. The intervening wires are not part of his house or office any more than are the highways along which they are stretched." *Id.* at 465.

120. *Id.* at 465–66.

121. *See* Camara v. Mun. Court, 387 U.S. 523, 528–29 (1967).

122. 389 U.S. 347, 351 (1967).

created a new safeguard for activities that took place outside the curtilage of the home.

III.
PRIVATE VERSUS PUBLIC SPACE

In 1967, the Supreme Court finally solidified around the arguments articulated in the dissents in *Olmstead* and *Goldman* and in dicta in *Silverman*, which recognized the impact of new technologies on privacy.[123] The Court overruled *Olmstead*, rejecting the idea that the reach of the Fourth Amendment "turn[ed] upon the presence or absence of a physical intrusion into any given enclosure."[124] More critical was whether individuals had a reasonable expectation of privacy.

In *Katz*, a gambler entered a public telephone booth, closed the door, and placed a call.[125] The privacy interests at stake could not be ignored. Justice Stewart explained on behalf of the Court, "The Government's activities in electronically listening to and recording the petitioner's words violated the privacy upon which [Katz] justifiably relied while using the telephone booth and thus constituted a 'search and seizure' within the meaning of the Fourth Amendment."[126] The central issue was not whether physical penetration of a constitutionally-protected area had occurred.[127] As Stewart famously articulated, "The Fourth Amendment protects people, not places."[128]

In his concurrence, Justice Harlan spelled out the two-part test that would henceforward be applied. First, whether an individual, by his or her conduct, had "exhibited an actual (subjective) expectation of privacy"[129] (or, as the majority articulated, whether he had demonstrated that "he seeks to preserve [something] as private.")[130] And, second, whether the subjective expectation was "one

123. *Compare id.*, *with Olmstead*, 277 U.S. at 438 (Brandeis, J., dissenting), *and* Goldman v. United States, 316 U.S. 129, 139 (1942) (Murphy, J., dissenting), *and* Silverman v. United States, 365 U.S. 505, 508–10 (1961).

124. *Katz*, 389 U.S. at 353.

125. *Id.* at 348, 352.

126. *Id.* at 353.

127. *Id.* ("The fact that the electronic device employed to achieve that end did not happen to penetrate the wall of the booth can have no constitutional significance.").

128. *Id.* at 351.

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

130. *Katz*, 389 U.S. at 351.

that society is prepared to recognize as 'reasonable.'"[131] The Court would look at the circumstances to ascertain whether an individual's expectation of privacy was justified.[132]

In *Katz*, the Court attempted to wrench Fourth Amendment doctrine from its tie to property rights, but it failed to deliver on its promise. The case left open myriad questions. Over the ensuing decade, the Court systematically worked its way through related areas, in the process modifying and carving out exceptions to the warrant requirement.[133] Simultaneously, the rules that evolved in the 1970s and '80s relied in significant measure on the physical world.[134] It was thus not Katz's reasonable expectation of privacy in his *communication*, per se, but his reasonable expectation of privacy *when he entered the phone booth* that proved central. The private/public distinction held. Current technologies, however, blur the distinction between private space and the public domain on which the court has relied as a way of understanding the interests at stake. Perhaps nowhere is this more apparent than in regard to location tracking.

A. Open Fields, Naked Eye

One of the earliest cases to reinforce the open fields doctrine came in 1974, when the Supreme Court determined that a Colorado inspector entering an individual's yard during the daytime to test the plumes of smoke being emitted from the homeowner's chimneys did not trigger Fourth Amendment protections.[135] In *Air Pollution Variance Board v. Western Alfalfa Corp.*, the Court went into great detail as to what had happened, concluding that the invasion of privacy, "if it can be said to exist, is abstract and theoretical."[136]

131. *Id.* at 361 (Harlan, J, concurring); *see also* Rakas v. Illinois, 439 U.S. 128, 143 n.12 (1978); United States v. White, 401 U.S. 745, 752 (1971) (plurality opinion); Smith v. Maryland, 442 U.S. 735, 740–41 (1979).

132. *Katz*, 389 U.S. at 361 (Harlan, J., concurring).

133. For application of the legitimate expectation of privacy test over the decade that followed *Katz,* see, for example, United States v. Chadwick, 433 U.S. 1, 11 (1977); United States v. Miller, 425 U.S. 435, 442–43 (1976); Couch v. United States, 409 U.S. 322, 335–36 (1976); United States v. Dionisio, 410 U.S. 1, 14 (1973); United States v. United States Court for E. Dist. of Mich., 407 U.S. 297, 313 (1972); *White*, 401 U.S. at 752; Mancusi v. DeForte, 392 U.S. 364, 368–69 (1968); Terry v. Ohio, 392 U.S. 1, 9 (1968).

134. *See* discussion, *infra*, Part III(A).

135. 416 U.S. 861, 865 (1974).

136. *Id.* ("The EPA regulation for conducting an opacity test requires the inspector to stand at a distance equivalent to approximately two stack heights away but not more than a quarter of a mile from the base of the stack with the sun to his back from a vantage point perpendicular to the plume; and he must take at least

A decade later, the Court reaffirmed its position in *Oliver v. United States*.[137] Hearkening back to *Hester*'s (pre-*Katz*) reliance on the text of the Fourth Amendment, the Court established that "effects" did not include "open fields."[138] In *Oliver*, the Kentucky State Police had received reports that a farmer was growing marijuana.[139] They searched Oliver's property, which was surrounded by a gate marked "No Trespassing," without first obtaining a warrant.[140] In a 6-3 decision, Justice Powell explained that the open fields doctrine applied.[141] Even where police officers might be engaged in a common law trespass, the act of entering a privately owned field did not automatically trigger Fourth Amendment protections.[142] Justice White's concurrence noted that fields, by definition, were neither a "house" nor an "effect."[143]

The Court recognized multiple factors for determining whether a place should be free from government intrusion absent a warrant.[144] It noted the importance of "the intention of the Framers of the Fourth Amendment, the uses to which the individual has put a location, and our societal understanding that certain areas deserve the most scrupulous protection from government invasion."[145] The factors were "equally relevant to determining whether the government's intrusion upon open fields without a warrant or probable cause violates reasonable expectations of privacy."[146]

The open fields doctrine applied even when the land in question was fenced and posted: "[A]n individual may not legitimately demand privacy for activities conducted out of doors in fields, except in the area immediately surrounding the home."[147] The Court emphasized "the overriding respect for the sanctity of the home

25 readings, recording the data at 15- to 30-second intervals. Depending upon the layout of the plant, the inspector may operate within or without the premises but, in either case, he is well within the 'open fields' exception to the Fourth Amendment approved in *Hester*.").

137. 466 U.S. 170 (1984).

138. *Id.* at 177.

139. *Id.* at 173.

140. *Id.* at 173–74.

141. *Id.* at 183–84.

142. *Id.* at 183–84.

143. *Oliver*, 466 U.S. at 184 (White, J., concurring).

144. *Id.* at 177–78.

145. *Id.* at 178 (citations omitted).

146. *Id.*

147. *Id.* By adopting this position, the court departed from the traditional understanding of curtilage, as the term had been used in criminal statutes and property disputes. *See generally* 1 CHITTY'S GENERAL PRACTICE 175 (London, Butterworth 1833).

that has been embedded in our traditions since the origins of the Republic."[148] Open fields, in contrast, did not provide a setting "for those intimate activities that the Amendment is intended to shelter from government interference or surveillance."[149]

Justice Marshall, joined by Justices Brennan and Stevens, dissented.[150] Marshall could not agree "that 'an individual may not legitimately demand privacy for activities conducted out of doors in fields, except in the area immediately surrounding the home.'"[151] The plain language of the amendment protected neither telephone booths nor businesses—yet both had fallen within its contours.[152] The reason was clear: the Fourth Amendment was not designed to specify with "precision" which activities were permissible or not, but rather "to identify a fundamental human liberty that should be shielded forever from government intrusion."[153] Unlike statutes, constitutional provisions must be understood in a way that "effectuate[s] their purposes—to lend them meanings that ensure that the liberties the Framers sought to protect are not undermined by the changing activities of government officials."[154] Marshall cited to Chief Justice Marshall's famous words in *McCulloch v. Maryland*, "[W]e must never forget, that it is a constitution we are expounding."[155] *Katz* had manifested this principle.[156]

Marshall argued that under a *Katz* analysis, the Court should look to positive law, the nature of the uses to which the space could be put, and whether the individual claiming the privacy interest made it clear to the public in a way that others "would understand and respect."[157] While privacy interests may not be coterminous with property rights, they reflected explicit recognition of a domain over which an individual held authority.[158] Marshall, nevertheless, fell back upon the traditional private/public distinction: "Privately owned woods and fields that are not exposed to public view regu-

148. *Oliver*, 466 U.S. at 178 (internal quotation marks omitted).

149. *Id.* at 179.

150. *Id.* at 184 (Marshall, J., dissenting).

151. *Id.* at 185 (Marshall, J., dissenting) (quoting *id.* at 178 (majority opinion)).

152. *Id.* at 185–86.

153. *Id.* at 186.

154. *Oliver*, 466 U.S. at 187.

155. *Id.* at 187 n.4 (Marshall, J., dissenting) (quoting McCulloch v. Maryland, 17 U.S. 316, 407 (1819)).

156. *Id.* at 187–88.

157. *Id.* at 189.

158. *Id.* at 189–90.

larly are employed in a variety of ways that society acknowledges deserve privacy."[159]

Oliver made it clear that *Katz* had not changed the basic tenets of the open fields doctrine. For the majority, it was not that *Katz* did not expand what might be included within a reasonable expectation of privacy. It simply did not incorporate open fields. For Marshall, the private/public distinction similarly controlled. He merely reached a different answer for privately owned land.[160]

Questions remained about the precise limits of the curtilage. In 1987, the Court went on to determine that the space immediately outside a barn—some half a mile from any road and only reachable after crossing a number of fences—constituted "open fields."[161] In *United States v. Dunn*, Robert Carpenter, and his co-defendant, Ronald Dunn, were convicted of conspiring to manufacture phenylacetone and amphetamine, as well as possessing amphetamine with an intent to distribute it.[162] Drug Enforcement Administration (DEA) agents discovered that Carpenter had purchased significant amounts of chemicals and equipment used in the manufacture of the controlled substances.[163] The agents obtained warrants from a Texas state judge, allowing them to install radio frequency-enabled transmitters in the material and equipment.[164] They tracked Carpenter's truck until it arrived at Dunn's ranch.[165] Aerial photographs captured images of the truck parked next to a barn.[166]

The property, some 198 acres, was encircled by a fence and contained several interior fences, mostly constructed of posts and barbed wire.[167] The nearest public road was a half-mile away.[168] A fence surrounded the house and a nearby greenhouse, with two barns another fifty feet away.[169] The front of one of the barns had a wooden fence around it, along with locked, waist-high gates and netting material stretched between the barn and the gates.[170] A DEA agent and an officer from the Houston Police Department

159. *Id.* at 192.
160. *Oliver*, 466 U.S. at 192.
161. United States v. Dunn, 480 U.S. 294, 303 (1987).
162. *Id.* at 296.
163. *Id.*
164. *Id.*
165. *Id.* at 297.
166. *Id.*
167. *Dunn*, 480 U.S. at 297.
168. *Id.*
169. *Id.*
170. *Id.*

crossed the outside fence and one interior fence.[171] Part way between the residence and the barns, the agent smelled phenylacetic acid coming from the barns.[172] The officers crossed another barbed-wire fence and a wooden fence, walked under the barn's overhang to the locked wooden gates, and, using a flashlight, looked into the barn.[173] Seeing a laboratory, they did not enter the barn, although the following day they returned twice to confirm their initial sighting.[174] That evening, they obtained a warrant authorizing them to search the ranch.[175] Two days later, they executed the warrant, seizing chemicals, laboratory equipment, and amphetamines.[176]

The Supreme Court reiterated the special place of the home in Fourth Amendment jurisprudence. "The curtilage concept," the Court wrote, "originated at common law to extend to the area immediately surrounding a dwelling house the same protection under the law of burglary as was afforded the house itself."[177]

The Court was right insofar as the curtilage had historically been considered relevant to the penalties associated with criminal activity. But it was not until 1928, with Taft's decision in *Olmstead*, that the term became drawn into the Supreme Court's Fourth Amendment jurisprudence. And prior to that time, curtilage had a much broader meaning.

According to Cunningham's law dictionary from 1764, for instance, curtilage meant precisely what the Court rejected in *Oliver*:

---

171. *Id.*

172. *Id.*

173. *Dunn*, 480 U.S. at 297–98.

174. *Id.* at 298.

175. *Id.*

176. *Id.* at 298–99. The District Court denied the defendants' motion to suppress evidence seized pursuant to the warrant—a decision later reversed by the Fifth Circuit in *United States v. Dunn*, 674 F.2d 1093 (5th Cir. 1982). The Supreme Court vacated the Fifth Circuit's judgment and remanded it for further consideration in light of *Oliver v. United States*, 466 U.S. 170 (1984). *Dunn*, 480 U.S. at 299. The Fifth Circuit again suppressed the evidence found in the course of the agents' first entry onto the premises—this time, not on the grounds that the barn was within the curtilage of the house but, rather, that by peering into the structure, the officers had violated Dunn's "reasonable expectation of privacy in his barn and its contents." *Id.* (internal quotation marks omitted). Before the Supreme Court entertained the petition for certiorari, the Fifth Circuit recalled and vacated its judgment and reinstated its original opinion, stating, "[u]pon studied reflection, we now conclude and hold that the barn was inside the protected curtilage." *Id.* (internal quotation marks omitted). The Supreme Court granted certiorari, and reversed the Fifth Circuit. *Id.* at 300.

177. *Dunn*, 480 U.S. at 300.

"a yard, backside, or piece of ground lying near a dwelling house, where they sow hemp, beans, and such like."[178] In 1820, Sheppard's *Touchstone of Common Assurances* described it as "a little garden, yard, field, or piece of void ground, lying near and belonging to the messuage, and houses adjoining the dwelling house, and the close upon which the dwelling-house is built."[179] In 1828, Johnson & Walker simply defined it as "a garden, yard, or field lying near to a messuage."[180]

Oliver narrowed the meaning of the term, and the Court in *Dunn* highlighted four factors to be taken into account:

> [T]he proximity of the area claimed to be curtilage to the home, whether the area is included within an enclosure surrounding the home, the nature of the uses to which the area is put, and the steps taken by the resident to protect the area from observation by people passing by.[181]

It eschewed a rigid adherence to the categories, arguing that they were "useful analytical tools only to the degree that, in any given case, they bear upon the centrally relevant consideration—whether the area in question is so intimately tied to the home itself that it should be placed under the home's 'umbrella' of Fourth Amendment protection."[182] Applied to the barn, the Court concluded that it did not.

Curtilage considerations thus dismissed, naked eye doctrine prevailed. "Under *Oliver* and *Hester*," the Court wrote, "there is no constitutional difference between police observations conducted while in a public place and while standing in the open fields."[183]

---

178. *Curtilage*, 1 TIMOTHY CUNNINGHAM, A NEW AND COMPLETE LAW DICTIONARY (London, Law-Printers to the King's Most Excellent Majesty 1764), https://archive.org/stream/newcompletelawdi01cunn#page/n613/mode/2up; *see also Curtilage*, 2 GILES JACOB & T.E. TOMLINS, THE LAW-DICTIONARY: EXPLAINING THE RISE, PROFESS, AND PRESENT STATE, OF THE ENGLISH LAW 171 (New York, I. Riley 1811) ("CURTILAGE, *curtilagrium*, from the Fr. *cour, court* and *Sax. leagh*, locus.] A court-yard, back-side, or piece of ground lying near and belonging to a dwelling house. And though it is said to be a yard or garden, belonging to a house, it seems to differ from a garden, for we find *cum quodam* gardino *et* curtilagio.") (citations omitted).

179. WILLIAM SHEPPARD & EDWARD HILLIARD, SHEPPARD'S TOUCHSTONE OF COMMON ASSURANCES 94 (London, 7th ed. 1820).

180. *Curtilage*, 1 Samuel Johnson & John Walker, A Dictionary of the English Language 176 (London, William Pickering 1827), https://books.google.com/books/about/A_Dictionary_of_the_English_Language.html?id=WBYwAAAAYAAJ.

181. *See Dunn*, 480 U.S. at 301 (discussing *Oliver* and deriving factors from lower courts).

182. *Id.*

183. *Id.* at 304.

Just as the observation from a plane in *California v. Ciraolo* (discussed *infra* in Section IIIB) did not violate the Fourth Amendment, neither did peering into the barn.[184] Despite *Katz's* move to a reasonable expectation of privacy as centered on persons, and not property, the curtilage of the home continued to serve as a proxy.

In *Dunn*, Justice Brennan, joined by Justice Marshall, dissented.[185] The reasoning paralleled their position in *Oliver*: the intrusion violated the Fourth Amendment because the barnyard "lay within the protected curtilage of Dunn's farmhouse," and the agents' inspection violated Dunn's reasonable expectation of privacy. Like the majority, the dissent's logic reflected the private-space/public domain distinction that had long marked Fourth Amendment doctrine. Brennan did note, though, the underlying *purpose* of the constitutional text: prohibiting "police activity which, if left unrestricted, would jeopardize individuals' sense of security or would too heavily burden those who wished to guard their privacy."[186] DEA agents had gone "one-half mile off a public road over respondent's fenced-in property, crossed over three additional wooden and barbed wire fences, stepped under the eaves of the barn, and then used a flashlight to peer through otherwise opaque fishnetting."[187] He concluded, "For the police habitually to engage in such surveillance—without a warrant—is constitutionally intolerable."[188]

Just a few months after *Dunn*, the Court beat the proverbial horse. In *California v. Greenwood*,[189] local police suspected Billy Greenwood of dealing drugs out of his home. Lacking sufficient evidence for a warrant, they searched his garbage and found inculpating material. In a 6-2 vote, the Court held that the garbage left out on the curb, "readily accessible to animals, children, scavengers,

184. In *Ciraolo*, the Court had observed that the Fourth Amendment "has never been extended to require law enforcement officers to shield their eyes when passing by a home on public thoroughfares." California v. Ciraolo, 476 U.S. 207, 213 (1986). Also note that in 1983 the court settled that simply using a flashlight to illuminate the interior of a car, without probable cause to search the automobile, did not transgress any rights secured by the Fourth Amendment. Texas v. Brown, 460 U.S. 730, 739–40 (1983); *see also* United States v. Lee, 274 U.S. 559, 563 (1927) (use of searchlight by Coast Guard on high seas is not a search).

185. *Dunn*, 480 U.S. at 305 (Brennan, J., dissenting).

186. *Id.* at 306.

187. *Id.* at 319.

188. *Id.*

189. California v. Greenwood, 486 U.S. 35 (1988).

snoops, and other members of the public," lay outside the protections of the Fourth Amendment.[190]

In his dissent, Justice Brennan, joined by Justice Marshall, emphasized that Greenwood had placed the garbage in opaque bags, blocking their view from casual passers-by.[191] Garbage could reveal a considerable amount about Greenwood's private life: "A single bag of trash testifies eloquently to the eating, reading, and recreational habits of the person who produced it," he wrote.[192] Search of the material could reveal "intimate details about sexual practices, health, and personal hygiene. Like rifling through desk drawers or intercepting phone calls, rummaging through trash can divulge the target's financial and professional status, political affiliations and inclinations, private thoughts, personal relationships, and romantic interests."[193] It reflected the type of "intimate knowledge associated with the 'sanctity of a man's home and the privacies of life'" that the Fourth Amendment was designed to protect.[194] The majority's private space/public domain distinction, premised on lesser expectations outside the physical borders of the home, had failed to capture the privacy interests at stake.

B. Aerial Surveillance

With the line still drawn post-*Katz* at the curtilage of the home, to the extent that new means of aerial surveillance raised privacy concerns, the Court dismissed them under the private/public distinction. The underlying rationale, that government officials should not be prevented from accessing what any citizen could see or hear, persisted.

In *California v. Ciraolo*, the police received an anonymous telephone tip that a resident of Santa Clara, California, was growing marijuana in his backyard.[195] A six-foot outer fence and a ten-foot inner fence blocked the view from the street, so the police hired a private plane to fly overhead.[196] They spotted marijuana plants, eight to ten feet tall, growing in a fifteen by twenty-five foot plot in the back yard.[197]

---

190. *Id.*
191. *See, e.g., id.* at 45 (Brennan, J., dissenting).
192. *Id.* at 50.
193. *Id.*
194. 486 U.S. 50–51 (Brennan, J., dissenting).
195. California v. Ciraolo, 476 U.S. 207, 209 (1986).
196. *Id.*
197. *Id.*

Chief Justice Burger, delivering the opinion of the Court, quickly dismissed the importance of the fence, noting that even the ten-foot-high structure "might not shield these plants from the eyes of a citizen or a policeman perched on the top of a truck or a two-level bus."[198]

Burger's statement was extraordinary, not least because it was *illegal* under California law for citizens to sit atop vehicles.[199] Nor were there, in 1982, *any* double-decker buses to be found in the largely rural and residential community.[200] Nevertheless, Burger suggested that any citizen could look over the fence from the top of a moving vehicle. It was therefore unclear whether the respondent had a subjective expectation of privacy or "merely a hope that no one would observe [the respondent's] unlawful gardening pursuits."[201]

Turning his attention to the curtilage, the Chief Justice noted that the common-law understanding was the area within which activities associated with the "sanctity of a man's home and the privacies of life" occurred.[202] "The protection afforded the curtilage," he wrote, "is essentially a protection of families and personal privacy in an area intimately linked to the home, both physically and psychologically, where privacy expectations are most heightened."[203] The yard, and its crops, *could* be understood as inside the curtilage.[204] But the burden was on the homeowner to ensure that the view was blocked.[205] The "naked-eye observation of the curtilage by police from an aircraft lawfully operating at an altitude of 1,000 feet" meant that the owner had not taken the requisite steps.[206] *Any* citizen, flying over the home within navigable airspace, could have seen the same thing.[207] The Fourth Amendment does not "require law enforcement officers to shield their eyes when passing by a

198. *Id.* at 211.

199. *See, e.g.*, 1981 Cal. Stat. 3, 155 (adding Subsection (b), stating that "No person shall ride on any vehicle or upon any portion thereof not designed or intended for the use of passengers," to Cal. Veh. Code §21712); 1982 Cal. Stat. 4, 709 (passed Sept. 22, 1982 making it illegal for a minor to be in the back of a flatbed truck, codified at Cal. Veh. Code §23116).

200. Author Note, having grown up in Santa Clara, California in the 1980s.

201. *Ciraolo*, 476 U.S. at 212.

202. *Id.* (quoting Oliver v. United States, 466 U.S. 170, 180 (1984)).

203. *Id.* at 212–13.

204. *Id.* at 213.

205. *See id.*

206. *Id.*

207. *Ciraolo*, 476 U.S. at 213–14.

home on public thoroughfares."[208] What was accessible to any person, had to be accessible to law enforcement.[209]

The decision was a 5-4 vote, with Justice Powell, joined by Justices Brennan, Marshall, and Blackmun, dissenting. Powell cited to Justice Harlan's warning in *Katz*, that tying the Fourth Amendment only to physical intrusion "is, in the present day, bad physics as well as bad law, for reasonable expectations of privacy may be defeated by electronic as well as physical invasion."[210] For the dissent, the airplane was "a product of modern technology" visually intruding into the respondent's yard.[211] While "[c]omings and goings on public streets are public matters," flying a plane over a home to conduct surveillance intrudes upon a reasonable expectation of privacy.[212]

Powell underscored the importance of the Fourth Amendment adapting to new and emerging technologies. "Rapidly advancing technology now permits police to conduct surveillance in the home itself," he explained, "an area where privacy interests are most cherished in our society, without any physical trespass."[213] Flexibility mattered. The Court had "repeatedly refused to freeze 'into constitutional law those enforcement practices that existed at the time of the Fourth Amendment's passage.'"[214] Instead, it had "construed the Amendment 'in light of contemporary norms and conditions,' . . . in order to prevent 'any stealthy encroachments' on our citizens' right to be free of arbitrary official intrusion."[215] By the time of *Ciraolo*, Powell noted, technological advances had "enabled police to see people's activities and associations, and to hear their conversations, without being in physical proximity."[216] The doctrine had to evolve to protect the privacy interests at stake.

The same day that the Court handed down *Ciraolo*, it issued an opinion in *Dow Chemical v. United States*, reinforcing the idea that what was visible in public was fair game.[217] Dow Chemical denied a

208. *Id.* at 213.

209. *Id.* at 213–14.

210. *Id.* at 215–16 (Powell, J., dissenting) (quoting Katz v. United States, 389 U.S. 347, 362 (1967) (Harlan, J., concurring)).

211. *Id.* at 222.

212. *Id.* at 224–25.

213. *Ciraolo*, 476 U.S. at 226 (Powell, J., dissenting).

214. *Id.* at 217 (Powell, J., dissenting) (quoting Steagald v. United States, 451 U.S. 204, 217 n.10 (1981)).

215. *Id.* (quoting *Steagald*, 451 U.S. at 217; Boyd v. United States, 116 U.S. 616, 635 (1886)).

216. *Id.* at 218.

217. Dow Chem. Co. v. United States, 476 U.S. 227 (1986).

request by the Environmental Protection Agency (EPA) to conduct an on-site inspection of a 2000-acre facility.[218] The EPA responded by hiring a commercial aerial photographer to take pictures of the facility from the air.[219]

Chief Justice Burger again wrote for the Court. He began the Fourth Amendment analysis by drawing a line between private and public space.[220] Activities undertaken potentially in the view of others did not deserve the same protections as those that transpired within the home.[221] While Dow Chemical held a "reasonable, legitimate, and objective expectation of privacy within the interior of its covered buildings" (one that society was prepared to recognize), it did not have an equally high expectation for areas exposed to aerial view.[222]

The Court emphasized the importance of not unduly hampering law enforcement. The photographs were "essentially like those commonly used in mapmaking. Any person with an airplane and an aerial camera could readily duplicate them."[223] It made no sense to force the government agency to close its eyes, to prevent it from seeing what anyone else could see and from memorializing the image with a photograph—as any citizen could do.[224]

In 1989, the Court went on to consider whether aerial surveillance from a helicopter just 400 feet above the ground similarly was exempt from Fourth Amendment protections.[225] The concept of the naked eye—and what other citizens would be able to do in the public realm—again figured largely in the decision.

Like the Santa Clara police in *Ciraolo*, a Florida county sheriff's office received an anonymous tip that Riley was growing marijuana in a greenhouse behind his home.[226] Located on five acres of property, his mobile home was surrounded by a fence, on which a sign

---

218. *Id.* at 229.

219. *Id.*

220. *Id.* at 235 ("The curtilage area immediately surrounding a private house has long been given protection as a place where the occupants have a reasonable and legitimate expectation of privacy that society is prepared to accept.") (citing *Ciraolo*, 476 U.S. at 207). Open fields, in contrast, "do not provide the setting for those intimate activities that the [Fourth] Amendment is intended to shelter from governmental interference or surveillance." *Id.* (alteration in original) (quoting Oliver v. United States, 466 U.S. 170, 179 (1984)).

221. *Id.* at 239.

222. *Id.* at 236, 239.

223. *Dow Chem. Co.*, 476 U.S. at 231.

224. *See id.*

225. Florida v. Riley, 488 U.S. 445, 447–48 (1989).

226. *Id.* at 448.

was posted saying, "DO NOT ENTER."[227] Unable to see behind the house from the street, an officer flew over the property in a helicopter.[228] The greenhouse had two sides enclosed and was covered with corrugated panels, some translucent and some opaque.[229] Two of the panels were missing.[230] The officer looked through the openings in the roof and the open sides of the greenhouse and saw the plants growing.[231] He used this information to obtain a search warrant, which yielded the plants.[232]

Justice White announced the judgment and wrote an opinion in which only three other justices joined.[233] Because Riley had left two sides of the greenhouse open, and had failed to cover the greenhouse entirely, he "could not reasonably have expected the contents of his greenhouse to be immune from examination by an officer seated in a fixed-wing aircraft flying in navigable airspace at an altitude of 1000 feet or . . . at an altitude of 500 feet, the lower limit of the navigable airspace for such aircraft."[234] It made no difference that the helicopter was at a height of 400 feet, as helicopters were not bound by the lower limits of navigable airspace as required for other aircraft. "Any member of the public could legally have been flying over Riley's property in a helicopter at the altitude of 400 feet."[235] Why force law enforcement to undertake a form of willful blindness?

Justice Brennan, joined by Justices Marshall and Stevens, dissented. Brennan disputed the plurality's focus on whether any member of the public could have conducted the activity undertaken by law enforcement, without also considering the difficulty of such activity and the frequency with which it was done by members of the public. "Is the theoretical possibility that any member of the public (with sufficient means) could also have hired a helicopter and looked over Riley's fence of any relevance at all in determining whether Riley suffered a serious loss of privacy . . . ?"[236] Law enforcement had not been standing on a public road.[237] "The vantage

227. *Id.*
228. *Id.*
229. *Id.*
230. *Id.*
231. *Riley*, 488 U.S. at 448.
232. *Id.* at 448–49.
233. *Id.* at 447 (joined by Chief Justice Rehnquist, Justice Scalia, and Justice Kennedy).
234. *Id.* at 450.
235. *Id.* at 451.
236. *Id.* at 457–58 (Brennan, J., dissenting).
237. *Riley*, 488 U.S. at 460 (Brennan, J., dissenting).

point he enjoyed," Brennan pointed out, "was not one any citizen could readily share."[238] To see over the fence, the officer had to use "a very expensive and sophisticated piece of machinery to which few ordinary citizens have access."[239] It made as much sense to rely on whether the officer was legally in the air, as it would have been to ascertain whether the police officers in *Katz* were legally standing outside the telephone booth.[240] "The question before us," Brennan explained, "must be not whether the police were where they had a right to be, but whether public observation of Riley's curtilage was so commonplace that Riley's expectation of privacy in his backyard could not be considered reasonable."[241]

Brennan's argument underscored the importance of focusing on the privacy interests implicated by new technologies. Yet largely because of the persistence of the private/public distinction, his arguments did not win the day. Warrantless searches and seizures inside a home may be presumptively unreasonable absent exigent circumstances.[242] But visual examination, even of areas inside the curtilage of the home, when conducted from a public sphere, lies outside the protections of the Fourth Amendment.[243]

C. Radio-frequency Enabled Transmitters

As technology progressed and questions relating to the reasonable expectation of privacy standard adopted in *Katz* arose, the Supreme Court held fast to its private/public distinction. Just as people had a lesser expectation of privacy in garbage placed curbside—indeed, no expectation whatsoever—so, too, did they outside of automobiles, as well as in their movements along public thoroughfares.[244]

---

238. *Id.*

239. *Id.*

240. *Id.*

241. *Id.*

242. *See* Welsh v. Wisconsin, 466 U.S. 740, 748–49 (1984); Steagald v. United States, 451 U.S. 204, 211–13 (1981); Payton v. New York, 445 U.S. 573, 586 (1980).

243. Precisely what constitutes the curtilage of the home continues to be a contentious issue in Fourth Amendment jurisprudence. *See* CLANCY, *supra* note 79, at § 4.4.1.1; 1 WAYNE R. LAFAVE, SEARCH AND SEIZURE: A TREATISE ON THE FOURTH AMENDMENT §2.3 (5th ed. 2016).

244. The seizure of a car travelling on a public highway, absent either probable cause or reasonable suspicion, did violate the Fourth Amendment. Delaware v. Prouse, 440 U.S. 648 (1979). In *Prouse*, a patrol officer stopped a car and smelled marijuana. *Id.* at 650. When the officer looked into the car, he saw the marijuana inside the vehicle. *Id.* Justice White, writing for the Court, stated, "An individual operating or traveling in an automobile does not lose all reasonable expectation of privacy simply because the automobile and its use are subject to government regu-

Thus it was in 1983, in *United States v. Knotts,* the Court confronted a case where Minnesota law-enforcement officers suspected Tristan Armstrong of stealing chemicals that could be used in manufacturing illicit drugs.[245] Visual surveillance revealed that he purchased chemicals from Hawkins Chemical Co. in Minnesota.[246] With the consent of company officials, when Armstrong next bought a container of chloroform (one of the precursor chemicals used to make drugs), the police placed a radio-frequency-enabled transmitter on the container.[247] The police followed the container, using the tracking device and visual surveillance, to a cabin in Wisconsin.[248] They obtained a search warrant and found a fully operable drug laboratory inside the cabin, replete with formulas for amphetamine and methamphetamine, $10,000 worth of equip-

---

lation." *Id.* at 662. He reasoned, "Automobile travel is a basic, pervasive, and often necessary mode of transportation to and from one's home, workplace, and leisure activities." *Id.* Since many people spent more time driving than walking, a higher degree of security might be felt in the car. *Id.* White continued, "Were the individual subject to unfettered governmental intrusion every time he entered an automobile, the security guaranteed by the Fourth Amendment would be seriously circumscribed." 440 U.S. 662–63.

Professor Clancy points to this case to suggest that the case served as an early indication that, following *Katz*, "privacy might be a vital source of protection of individual interests." CLANCY, *supra* note 79, at § 3.3.3. He argues, "as the composition of the Court changed," however, "those early indications gave way to a view that used privacy analysis not to expand protected individual interests but to limit the scope of the Amendment's protections." *Id.* What emerged was a "hierarchy of privacy interests." *Id.* Amongst the lowest level of protection is an individual's voice, face, or handwriting, as well as travel and open fields. *Id.*

The hierarchy that Clancy identifies, though, relies on the private/public distinction as the defining feature. Lowered protections accompanied what could be seen and observed by others in public space. Clancy treats whether something is observable as only one of several potential methods adopted by the Court to distinguish between privacy interests, noting also the degree to which technological advances, empirical evidence of a subjective expectation of privacy, and degree of government regulation. *Id.* at § 3.3.4. This Article takes the stronger position, which is that the private/public distinction is a central feature of the doctrine, which remains rooted in a terrestrial understanding of a three-dimensional world, making it ill-suited to confront the challenges of a digital age.

245. United States v. Knotts, 460 U.S. 276, 278 (1983); *cf.* United States v. Michael, 622 F.2d 744 (5th Cir. 1980) (holding that installation of a beeper, absent probable cause and exigent circumstances, required prior judicial authorization), *reh'g granted*, 628 F.2d 931 (5th Cir. 1980), *rev'd*, 645 F.2d 252 (5th Cir. 1981) (finding the installation of the beeper permissible under the Fourth Amendment using a reasonable suspicion standard).

246. *Knotts*, 460 U.S. at 278.

247. *Id.*

248. *Id.*

ment, and enough chemicals to produce 14 pounds of pure amphetamine.[249]

The Eighth Circuit reversed the conviction on the grounds that monitoring the radio-frequency-enabled transmitter violated the cabin owner's reasonable expectation of privacy.[250] The Supreme Court disagreed and reversed.[251] In an opinion written by Chief Justice Rehnquist, the Court analyzed the question in terms of the open fields/naked eye doctrine. The transmitter was merely a battery-operated device, emitting periodic signals that could be picked up by a receiver. It allowed law enforcement to do electronically what it could do in person "on public streets and highways."[252]

Rehnquist picked up on the 1974 language in *Cardwell v. Lewis*, which stated: "A car has little capacity for escaping public scrutiny. It travels public thoroughfares where both its occupants and its contents are in plain view."[253] In *Knotts*, Rehnquist argued, "A person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another."[254] The direction they took, stops they made, and their final destination could be observed.[255] Just because the police relied on a radio-frequency-enabled transmitter, and not their own eyes, did not alter the situation. Rehnquist explained, "Nothing in the Fourth Amendment prohibited the police from augmenting the sensory faculties bestowed upon them at birth with such enhancement as science and technology afforded them in this case."[256]

The respondent argued that if the Court were to adopt this rule, then there would be no limiting condition on the eventual use of 24-hour surveillance.[257] The Court disagreed, suggesting that technology, in reality, was nowhere near that point. "[I]f such drag-

249. *Id.* at 279.

250. *Id.* (discussing the case below, United States v. Knotts, 662 F.2d 515 (8th Cir. 1983)).

251. *Id.* at 279–80.

252. *Knotts*, 460 U.S. at 281.

253. *Id.* at 281 (quoting Cardwell v. Lewis, 417 U.S. 583, 590 (1974) (plurality opinion) (holding the warrantless search of the outside of a car to be outside the contours of the Fourth Amendment)) (also citing Rakas v. Illinois, 439 U.S. 128, 153–54 (1978) (Powell, J., concurring); South Dakota v. Opperman, 428 U.S. 364, 368 (1976)).

254. *Knotts*, 460 U.S. at 281.

255. *Id.* at 281–82.

256. *Id.* at 282; *see also id.* at 282–83 (discussing United States v. Lee, 274 U.S. 559, 563 (1927) (finding that the use of a searchlight is comparable to the use of a marine glass or field glass and thus does not change the analysis of the reasonableness of a search on the high seas)).

257. *Id.* at 283.

net-type law enforcement practices as respondent envisions should eventually occur, there will be time enough then to determine whether different constitutional principles may be applicable."[258] Radio-frequency-enabled transmitters, also known as "beepers," were merely "a more effective means of observing what is already public."[259]

The following year the Court confronted a similar fact pattern in *United States v. Karo*.[260] The DEA had learned that James Karo and two others had ordered 50 gallons of ether to be used to extract cocaine from clothing that had been imported to the United States.[261] Agents traced the container inside a number of homes, before tracking it to a commercial storage facility.[262]

Unlike *Knotts*, where the transmitter conveyed the location of a car on public roads, in *Karo* the beeper informed the agent where a container was located, at a particular time and, consequently, in whose possession it was held: i.e., the person(s) whose residence was under surveillance. "Even if visual surveillance has revealed that the article to which the beeper is attached has entered the house, the later monitoring not only verifies the officers' observations but also establishes that the article remains on the premises."[263] The search was less intrusive than a full-scale search, but it was still a search of the interior of the home. It therefore fell *within* the protections of the Fourth Amendment.[264] The private/public distinction, and the importance of maintaining access for acquiring visual information, held. Where law-enforcement collection techniques crossed the curtilage, constitutional protections arose.

The ordinary operation of the senses continued to loom large in the Court's jurisprudence.[265] What individuals could observe in

258. *Knotts*, 460 U.S. at 284.

259. *Id.* (quoting United States v. Knotts, 662 F.2d 515, 518 (8th Cir. 1983)); *see also id.* at 285.

260. 468 U.S. 705, 707–10 (1984).

261. *Id.* at 708.

262. *Id.*

263. *Id.* at 715.

264. *Id.* at 716.

265. The importance of the naked eye, for instance, extends to the plain view doctrine. In *Coolidge v. New Hampshire,* the Supreme Court explained that under certain circumstances seizure of an item in plain view during a lawful search may be reasonable under the Fourth Amendment. 403 U.S. 443, 465 (1971). Three elements must be met: (1) the officer must be lawfully in the Fourth Amendment-protected area; (2) the item observed must be in plain view; and (3) the officer must immediately recognize the item as illegal materials, evidence, or contraband without otherwise interfering with the item. Horton v. California, 496 U.S. 128, 136–37 (1990). In *Arizona v. Hicks*, the Court further elaborated on what consti-

public fell outside the protections of the Fourth Amendment. Law enforcement officers should not be forced to avert their gaze to block out what the rest of the world could see.

The functional-senses test included not just what individuals could see but also what they could hear without technological assistance. A 1984 case from the Second Circuit, *United States v. Mankani*, reflected this approach.[266] Canadian law enforcement uncovered a drug-running operation that yielded nearly two tons of hashish in a barn in a rural area of Vermont.[267] Having been tipped off by Canadian authorities that two of the men involved in the shipment were in a hotel room in Burlington, a DEA agent booked the adjoining room and listened through a hole in the wall to the conversation next door.[268] The Court concluded that eavesdropping did not violate the Fourth Amendment: "[D]efendants' conversations were overheard by the naked human ear, unaided by any . . . sensory enhancing devices. This distinction is significant because the Fourth Amendment protects conversations that cannot be heard except by means of artificial enhancement."[269] Every time individuals spoke, they assumed the risk that someone might be privy to what they say.[270] On the other hand, once technology enhanced the senses, then the risk altered. As Justice Brennan had expressed in his dissent in *Lopez v. United States*, "There is no security from that kind of eavesdropping, no way of mitigating the risk, and so not even a residuum of true privacy."[271]

Passive observation proved central to the functional senses approach. What one could see or hear, just standing there, was not

---

tuted an interference under condition (c). In that case, moving and then recording the serial numbers on the bottom of a stolen stereo did not amount to a seizure, but it was a search under the Fourth Amendment. Justice Scalia, writing for the Court, explained that "taking action, unrelated to the objectives of the authorized intrusion, which exposed to view concealed portions of the apartment or its contents, did produce a new invasion of respondent's privacy unjustified by the exigent circumstance that validated the entry." 480 U.S. 321, 325 (1987). Because the officer lacked "probable cause to believe that the equipment was stolen," the action fell outside plain-view doctrine. *Id.* at 326.

266. 738 F.2d 538 (2d Cir. 1984).

267. *Id.* at 541; *see also* United States v. Agapito, 620 F.2d 324 (2d Cir 1980) (listening by placing one's ear against an adjoining door does not violate the Fourth Amendment), *cert. denied*, 449 U.S. 834 (1980).

268. *Mankani*, 738 F.2d at 541.

269. *Id.* at 543; *see also* 1 WAYNE LAFAVE, SEARCH AND SEIZURE: A TREATISE ON THE FOURTH AMENDMENT § 2.2, at 270–72 (1st ed. 1978).

270. Hoffa v. United States, 385 U.S. 293, 303 (1966).

271. Lopez v. United States, 373 U.S. 427, 466 (1963) (Brennan, J., dissenting); *see also* discussion *infra* Part III(F)(2).

protected. But if a search involved physical manipulation, such as opening a bag, squeezing it, or feeling its contours, then the ordinary senses test did not apply.[272]

D. Global Positioning System Technology

GPS technology is similar to the radio frequency beepers used in *Knotts* and *Karo* in that it allows law enforcement to monitor the movements of one or more persons or objects, from a remote location, for some amount of time.[273] But it differs in terms of accuracy, reliability, the verification required (impacting resources required for monitoring the device, the likelihood of detection, and the degree of intrusion), the level of detail obtained, and the potential analytical yield.[274] A brief discussion of these five characteristics provides context for the types of privacy concerns raised the 2012 case of *United States v. Jones*.[275]

First, GPS devices are more accurate than beepers. GPS can pinpoint where a tracked device is located to within a few centimeters.[276] In contrast, radio-frequency transmitters appear to provide

---

272. *See, e.g.*, Bond v. United States, 529 U.S. 334, 337 (2000) (responding to the government's claim "that by exposing his bag to the public, petitioner lost a reasonable expectation that his bag would not be physically manipulated," by noting that *Ciraolo* and *Riley* "involved only visual, as opposed to tactile, observation.").

273. *See* Reneé McDonald Hutchins, *Tied Up in Knots? GPS Technology and the Fourth Amendment*, 55 UCLA L. REV. 409, 415 (2007).

274. *See generally* April A. Otterburg, Note, *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, 681–82 (2005) (discussing State v. Jackson, 76 P.3d 217 (Wash. 2003)); Hutchins, *supra* note 273, at 418–19; Brief of Appellants at 57, United States v. Jones, 615 F.3d 544 (D.C. Cir. 2010) (No. 08–3030), 2009 WL 3155141 [hereinafter: Appellants' Brief]; Ian Herbert, Note, *Where We Are with Location Tracking: A Look at the Current Technology and the Implications on Fourth Amendment Jurisprudence*, 16 BERKELEY J. CRIM. L. 442 (2011).

275. United States v. Jones, 132 S. Ct. 945 (2012).

276. Derek Major, *Another Great Leap for GPS?*, GCN (Feb. 17, 2016), https://gcn.com/articles/2016/02/17/improved-gps.aspx?s=gcntech_180216. In 1978, the Department of Defense launched its first GPS satellite. Darren Griffin, *How Does the Global Positioning System Work?*, POCKETGPSWORLD.COM, http://www.pocketgpsworld.com/howgpsworks.php (last updated June 26, 2011). By 1994, the system had expanded to include 24 satellites, collectively called NAVSTAR. SCOTT PACE ET AL., RAND CORP., THE GLOBAL POSITIONING SYSTEM: ASSESSING NATIONAL POLICIES 246 (1995). The system now includes approximately 30 satellites that orbit the Earth at an altitude of 20,000 kilometers. *How Does GPS Work?*, PHYSICS.ORG, http://www.physics.org/article-questions.asp?id=55 (last visited Nov. 19, 2016). Although it initially reserved the system for the military, in May 2000, the U.S. government opened it to civilian use. Press Release, Office of the Press Secretary of the White House, Statement by the President Regarding the United States' Decision to Stop Degrading Global Positioning System Accuracy

only a general location.[277] The distinction means that more accu-

(May 1, 2000), https://clinton4.nara.gov/WH/EOP/OSTP/html/0053_2.html. The decision proved essential to private sector innovation. By 2003, the technology had exploded to support a $4.7 billion market. NATIONAL WORKRIGHTS INSTITUTE, ON YOUR TRACKS: GPS TRACKING IN THE WORKPLACE 5 (2004). Uses ranged from employers wanting to track their workers by installing GPS chips on vehicles, in badges, and on phones, to law enforcement using the information as part of criminal investigations. *Id.* at 10–15.

NAVSTAR continues to evolve. On February 5, 2016, the Air Force successfully launched the final GPS IIF satellite. *Space Segment*, GPS.GOV, http://www.gps.gov/systems/gps/space/#IIF (last updated Oct. 4, 2016). The solicitation process for GPS III space vehicles, moving NAVSTAR to its third iteration, has already begun. Space and Missile Systems Center, *SMC Releases RFP for GPS III Space Vehicles 11+ Phase 1 Production Readiness Feasibility Assessment*, AIR FORCE SPACE COMMAND (Jan. 8, 2016), http://www.afspc.af.mil/News/Article-Display/Article/730920/smc-releases-rfp-for-gps-iii-space-vehicles-11-phase-1-production-readiness-fea.

NAVSTAR has proven important not just within the United States but worldwide. The only current global alternative is the Russian-Operated Global Navigation Satellite System (GLONASS). Chris Bergin & William Graham, *Soyuz 2-1B Launches Latest GLONASS-M Spacecraft*, NASASPACEFLIGHT.COM (Feb. 6, 2016), http://www.nasaspaceflight.com/2016/02/soyuz-2-1b-latest-glonass-m-spacecraft/. The European Union recently initiated a navigation satellite system for Europe, entitled Galileo, which is interoperable with NAVSTAR and GLONASS. *What Is Galileo?*, EUROPEAN SPACE AGENCY, http://www.esa.int/Our_Activities/Navigation/Galileo/What_is_Galileo (last updated Dec.18, 2015). The EU launched the first two satellites in October 2012 to validate the concept. Two more followed nearly a year later. Four pairs of fully operational capability satellites have since been launched, through December 17, 2015. When fully deployed, the system will have 24 operational satellites positioned in three circular medium earth orbit planes, approximately 23,000 kilometers above the surface. They are expected to be available by the end of 2016, with completion slotted for 2020. *Id.* The People's Republic of China, which currently operates the regional Beidou Navigation Satellite System, plans to expand it into a global system by 2020. El Borromeo, *China to Unveil 40 Beidou Navigation Satellites in Five Years: Spokesperson*, YIBADA (Feb. 6, 2016), http://en.yibada.com/articles/102630/20160206/china-unveil-40-beidou-navigation-satellites-five-years-spokesperson.htm. India, Japan, and France all run or are developing regional systems. Deepu Madhavan, *Say Goodbye to GPS! India's All Set to Switch to the Desi Navigation System, IRNSS*, INDIA TIMES (Dec. 8, 2015), http://www.indiatimes.com/news/india/say-goodbye-to-gps-india-s-all-set-to-switch-to-the-desi-navigation-system-called-indian-regional-navigation-satellite-system-irnss-248186.html; *What is the Quasi-Zenith Satellite System?*, NATIONAL SPACE POLICY SECRETARIAT OF JAPAN, http://qzss.go.jp/en/overview/services/sv02_why.html (last visited Nov. 19, 2016); HONBO ZHOU, THE INTERNET OF THINGS IN THE CLOUD: A MIDDLEWARE PERSPECTIVE 130 (2013) (noting that France is developing a regional system).

277. In its reply brief in *Karo*, the government stated that law enforcement officers standing on a sidewalk 25-50 feet from a home could tell whether the beeper was located in the front or back of the home, or on the right or left side. Clifford S. Fishman, *Electronic Tracking Devices and the Fourth Amendment:* Knotts, Karo, *and the Questions Still Unanswered*, 34 CATH. U. L. REV. 277, 282 (1985) (citing

rate data can be obtained from GPS, providing deeper insight into the individual or object under surveillance.

Second, GPS data is more reliable: beepers cannot be used in inclement weather, whereas GPS operates regardless of whether it is sunny, raining, or the middle of a blizzard.[278] Thus for GPS, the amount (and quality) of data is not limited by natural conditions.

Third, the two systems depart in what must be done to verify the information. GPS allows for law enforcement to be located virtually anywhere.[279] For a radio-frequency transmitter, the police have to be relatively nearby.[280] This has several implications.

For one, it takes a considerable amount of manpower, equipment, and resources to conduct surveillance using a beeper, whereas the costs for using GPS are lower.[281] From a resource perspective, therefore, law enforcement officers could entertain a lower level of individual suspicion before placing an individual under surveillance using GPS than might otherwise be the case for their decision to employ radio-frequency chips. Similarly, using GPS, they could choose to put multiple people under surveillance simultaneously, resulting in greater inroads into privacy because of the lowered resource commitment entailed.

For another, since police need to be nearby, drivers are more likely to be able to detect police tracking a beeper than police following GPS data.[282] The absence of any observable government presence may have implications for the relationship of citizens to the government, as the surreptitious nature of the surveillance raises question about the extent of government activity.[283] To the

---

Reply Brief for Petitioners at 9 n.6, United States v. Karo, 468 U.S. 705 (1984) (No. 83–850)).

278. Hutchins, *supra* note 273, at 418; Appellants' Brief, *supra* note 274, at 57.

279. Scott W. Turner, *GPS Surveillance, the Right to Privacy, and the Fourth Amendment*, 40 COLO. LAW. 55, 57 (2011) ("Much like [radio beepers] . . . a GPS unit can be placed on an object and observed as it is being moved. The observation can be continuous. However, because of the technology, a person does not have to be nearby to obtain its signal. The movement of an individual being tracked through a GPS device can be observed by someone sitting at a computer from essentially anywhere.").

280. In *Karo*, the government stated that under ordinary conditions on the open road, the signal could be monitored 2-4 miles away, and up to 20 miles in the air. Once a beeper went inside premises, however, it was not always possible to identify its location. Fishman, *supra* note 277, at 282 (citing Reply Brief, *supra* note 277, at 8 n.6).

281. Appellants' Brief, *supra* note 274, at 57.

282. *Id.*

283. *See, e.g.*, Herbert, *supra* note 274, at 458–60 (discussing a number of incidents where individuals discovered FBI GPS surveillance devices on their cars).

extent that law enforcement agencies state that any information about GPS devices or tracking technologies is "law enforcement sensitive" (and thus refuse to release any information publicly about their use of the technologies), the concern increases.[284]

In addition, because radio-frequency enabled transmitters require the police to be in close proximity, officers cannot easily follow the person or object onto private land, within gated communities, or across borders.[285] In contrast, a GPS device may be carried virtually anywhere, including the most intimate spheres of personal and family life, without the target knowing that the information is being collected and monitored by the government. GPS data obtained on multiple people also can be correlated, showing others with whom the individual is sharing those spaces, generating insight into intimate relationships.

Fourth, GPS chips provide more detailed information than can be obtained from beepers.[286] GPS generates location data on a second-by-second basis. And it is automated, so the government can turn it on and then more or less ignore it. It can record information indefinitely, until law enforcement officials (or anyone else with access to the system) would like to look at the data, or to find (in real time) the person or object being tracked.[287] In contrast, in addition to being less accurate than GPS chips, beepers only send out periodic signals, generating smaller amounts of information. Someone has to be present to pick up the information, so less of it is captured. And beepers are only good for as long as their battery has power.

Fifth, because GPS data is detailed and digital, law enforcement can more easily combine it with other data, and synthesize and analyze an individual's movement over lengthy periods,[288] even predicting, based on pattern analytics, the individual's *future* movements. This is more than just ordinary sensory perception, to which Fourth Amendment doctrine clings. It introduces a different form of knowledge acquisition than is at stake in radio-frequency enabled transmitter tracking.[289]

---

284. *Id.* at 459–61.

285. Appellants' Brief, *supra* note 274, at 57.

286. *Id.*

287. *See* Hutchins, *supra* note 273, at 458; *see also* Appellants' Brief, *supra* note 274, at 57, 64.

288. Appellants' Brief, *supra* note 274, at 57.

289. *See, e.g.*, State v. Jackson, 76 P.3d 217, 223 (Wash. 2003) ("We perceive a difference between the kind of uninterrupted, 24-hour a day surveillance possible through use of a GPS device, which does not depend upon whether an officer

In sum, compared to beepers, GPS technology is more accurate and more reliable. It requires fewer resources and is harder to detect. It provides enormous detail and can be analyzed and combined with other information to generate further insight into suspects' lives. Law enforcement has therefore become increasingly reliant on GPS data for investigations.[290] An increasing number of cases are therefore coming before the courts, challenging the warrantless use of GPS technology.

Much like the Court in *Olmstead*, when confronted by telephone communications, a number of lower courts initially treated the placement of GPS chips on vehicles consistent with the *Knotts* framework, finding that it did not constitute a search.[291] Satellite-based tracking fell on the same side of the line as surveillance cameras and satellite imaging.[292]

A few courts, however, disagreed.[293] In 2003, the state of Washington determined that, unlike binoculars or a flashlight, GPS systems did not merely enhance the natural senses.[294] They provided a substitute for visual tracking, resulting in significant intrusions into individuals' private affairs.[295] The text of the Washington state constitution mattered: "no person shall be disturbed in his private af-

---

could in fact have maintained visual contact over the tracking period, and an officer's use of binoculars or a flashlight to augment his or her senses.").

290. *See* ALISON M. SMITH, CONG. RESEARCH SERV., R41663, LAW ENFORCEMENT USE OF GLOBAL POSITION (GPS) DEVICES TO MONITOR MOTOR VEHICLES: FOURTH AMENDMENT CONSIDERATIONS 1–3 (2011).

291. *See, e.g.*, United States v. Cuevas-Perez, 640 F.3d 272, 273, 275–76 (7th Cir. 2011) (finding 60-hour GPS surveillance outside the protections of the Fourth Amendment), *cert. granted and judgment vacated*, 132 S. Ct. 1534 (2012); United States v. Pineda-Moreno, 591 F.3d 1212, 1217 (9th Cir. 2010), *cert. granted and judgment vacated*, 132 S. Ct. 1533 (2012); United States v. Marquez, 605 F.3d 604, 609–10 (8th Cir. 2010); United States v. Garcia, 474 F.3d 994, 997 (7th Cir. 2007) (holding that GPS simply uses technology to substitute for trailing a car on a public street, which does not amount to a search within the meaning of the Fourth Amendment); United States v. McIver, 186 F.3d 1119, 1125 (9th Cir. 1999), *cert. denied*, 528 U.S. 1177 (2000); United States v. Moran, 349 F. Supp. 2d 425, 467 (N.D.N.Y. 2005) (holding use of a GPS device to be within the automobile exception); Osburn v. State, 44 P.3d 523 (Nev. 2002) (applying State constitution).

292. *Garcia*, 474 F.3d at 997.

293. *See, e.g.*, United States v. Maynard, 615 F.3d 544, 555–56 (D.C. Cir. 2010) (tracking movements for twenty-four hours a day for four weeks by GPS is a search); People v. Lacey, No. 2463N/02, 787 N.Y.S.2d 680, 2004 WL 1040676, at *8 (Nassau Cty. Ct. N.Y. May 6, 2004) (unpublished table opinion), *aff'd*, 787 N.Y.S.2d 680 (N.Y. App. Div. 2009); State v. Campbell, 759 P.2d 1040 (Or. 1988) (applying State constitution and finding that use of radio transmitter to locate automobile was a search); *Jackson*, 76 P.3d 217.

294. *Jackson*, 76 P.3d at 223.

295. *Id.*

fairs, or his home invaded, without authority of law."[296] The Washington Supreme Court noted that the insight into individuals' private lives that can be gleaned by GPS data is substantial:

> For example, the device can provide a detailed record of travel to doctors' offices, banks, gambling casinos, tanning salons, places of worship, political party meetings, bars, grocery stores, exercise gyms, places where children are dropped off for school, play, or day care, the upper scale restaurant and the fast food restaurant, the strip club, the opera, the baseball game, the "wrong" side of town, the family planning clinic, the labor rally.[297]

Such information could provide details on citizens' preferences, associations, and predilections, drawing a "detailed picture of one's life."[298]

The Washington court was not alone. In *People v. Lacey*, a New York court similarly determined that law enforcement use of a GPS device required a warrant.[299] In that case, a woman returned home to find two men at her back door.[300] She chased them and took down the license plate of the black 1996 Mitsubishi Eclipse they were driving.[301] Another incident in the same county occurred involving a black Mitsubishi, (along with a series of other local burglaries), prompting the detective in charge of the investigation to request permission from his lieutenant to place a GPS device on the car.[302] The police then tracked the vehicle, correlated its location with a number of burglaries, and arrested the owner in the middle of a heist.[303]

---

296. WASH. CONST. art. 1, § 7, *construed in Jackson*, 76 P.3d at 222 ("The inquiry under article 1, section 7 is broader than under the Fourth Amendment to the United States Constitution.").

297. *Jackson*, 76 P.3d at 223.

298. *Id.*

299. People v. Lacey, No. 2463N/02, 787 N.Y.S.2d 680, 2004 WL 1040676, at *8 (Nassau Cty. Ct. N.Y. May 6, 2004) (unpublished table opinion), *aff'd*, 787 N.Y.S.2d 680 (N.Y. App. Div. 2009).

300. *Id.* at *1.

301. *Id.*

302. *Id.* at *1–*2.

303. *Id.* at *3. As the question of whether the Fourth Amendment applied to GPS devices was a case of first impression for New York, the court looked to other state cases for guidance. *Id.* at *5–*6, (citing, among others, State v. Jackson, 76 P.3d 217 (Wash. 2003); State v. Campbell, 759 P.2d 1040 (Or. 1988); Johnson v. State, 492 So. 2d 693, 694 (Fla. Dist. Ct. App. 1986) (holding that a beeper on a plane was "tantamount to an illegal entry and beyond the scope of the warrant")). However, the court in *Lacey* mentioned, although it did not discuss in detail, a number of cases that went the other way. 2004 WL 1040676, at *6–*7 (citing,

The court balked at the possibility that the police could place GPS devices on vehicles and follow them around indefinitely without probable cause. "The citizens of New York," Judge Joseph Calabrese stated, "have the right to be free in their property, especially in light of technological advances which have and continue to diminish this privacy."[304] If it were a telephone communication, the police would have to obtain a warrant: "While the telegraph has become a relic of the past, cellular technology has become the future."[305] The judge was concerned about what the future might hold:

> At this time, more than ever, individuals must be given the constitutional protections necessary to their continued unfettered freedom from a "big brother" society. Other than in the most exigent circumstances, a person must feel secure that his or her every movement will not be tracked except upon a warrant based on probable cause establishing that such person has been or is about to commit a crime. Technology cannot abrogate our constitutional protections.[306]

In *Lacey*, Judge Calabrese boldly addressed the key question—an opportunity the Supreme Court failed to take, more than a decade later.[307]

In *United States v. Jones*, the Court considered a GPS chip that the police placed on the car of a suspected drug dealer's wife and monitored for 28 days.[308] Justice Scalia, writing for the Court, stated that the placement of the chip on the car, which occurred outside the period allowed by the warrant, amounted to a trespass.[309] Scalia distinguished *Karo*, noting that what made the placement of the

---

among others, State v. Clifton, 580 S.E.2d 40 (N.C. Ct. App. 2003) (upholding the constitutionality of law enforcement use of a manufacturer-installed GPS); Whitehead v. State, 574 S.E.2d 351 (Ga. Ct. App. 2002) (affirming conviction where police placed a GPS device on an informer's car, with the informer's consent)).

304. *Lacey*, 2004 WL 1040676, at *8.

305. *Id.*

306. *Id.*

307. *See* United States v. Jones, 132 S. Ct. 945, 954 (2012). In addition to a number of state court decisions, a number of state legislatures have taken steps to prohibit the warrantless use of electronic tracking devices; *see also* Herbert, *supra* note 274, at 445 nn.12–14 (citing laws passed in Utah, Florida, South Carolina, Oklahoma, Hawaii, Pennsylvania, and California).

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

309. *Id.* at 352; *see also* Johnson v. State, 492 So. 2d 693, 694 (Fla. Dist. Ct. App. 1986) (holding that installation of a beeper inside a plane amounted to an illegal entry and thus a violation of the Fourth Amendment); People v. Oates, 698 P.2d 811, 816 (Colo. 1985) (en banc) (applying State constitution and finding that placement of a beeper inside a container of chemicals after the defendant had

transmitter in the container of ether legal was that it was placed into the device *before* the target of the surveillance had possession. In contrast, the car was already in Antoine Jones's wife's possession when law enforcement attached the device.[310] He reasoned that the case was entirely consistent with *Knotts*; the holding in *Knotts* merely recognized that the target had no reasonable expectation of privacy, per *Katz*, in the location of the automobile carrying the container of chloroform.[311] *Katz*, however, had to be understood as adding to, not substituting for, the common law trespassory test. As in *Karo*, "The beeper had been placed in the container before it came into Knotts' possession, with the consent of the then-owner."[312]

Scalia reiterated that naked eye doctrine controls public space. "This Court has to date not deviated from the understanding that mere visual observation does not constitute a search."[313] What one could ascertain from ordinary senses, in public, lay beyond the reach of the Fourth Amendment. He went on to reject any privacy interest in the length of the surveillance. "[E]ven assuming that the concurrence is correct to say that '[t]raditional surveillance' of Jones for a 4-week period 'would have required a large team of agents, multiple vehicles, and perhaps aerial assistance,' . . . our cases suggest that such visual observation is constitutionally permissible."[314] At the same time, he admitted that the Court might have to grapple with the implications of lengthy surveillance in the future: "It may be that achieving the same result through electronic means, without an accompanying trespass, is an unconstitutional invasion of privacy, but the present case does not require us to answer that question."[315]

While Scalia sidestepped the hard questions presented by persistent monitoring, Justice Alito, joined in his concurrence by Justice Ginsburg, Justice Breyer, and Justice Kagan, did not.[316] Alito began by drawing a parallel between the majority in *Jones* and the Court in *Silverman*, which (consistent with *Olmstead*) had required "unauthorized physical penetration" for Fourth Amendment inter-

---

partially purchased and taken possession of the materials amounted to a warrantless search).

310. *Jones*, 132 S. Ct. at 952.

311. *Id.* at 951–52.

312. *Id.* at 952.

313. *Id.* at 953.

314. *Id.* at 953–54 (citation omitted) (quoting *id.* at 963 (Alito, J., concurring)).

315. *Id.* at 954.

316. *Jones*, 132 S. Ct. at 958 (Alito, J., concurring).

ests to arise.[317] The *Jones* majority similarly focused on physical intrusion, despite the fact that, post-*Katz*, the trespass rule no longer applied.[318] For Alito, the key question was whether the long-term monitoring of the car violated the respondent's reasonable expectation of privacy.[319] He concluded that it did.[320] Technology, Alito averred, can change expectations.

> Recent years have seen the emergence of many new devices that permit the monitoring of a person's movements. In some locales, closed-circuit television video monitoring is becoming ubiquitous. On toll roads, automatic toll collection systems create a precise record of the movements of motorists who choose to make use of that convenience. Many motorists purchase cars that are equipped with devices that permit a central station to ascertain the car's location at any time . . . . Perhaps most significant, cell phones and other wireless devices now permit wireless carriers to track and record the location of users.[321]

Limited resources previously played a role in restricting incursions into privacy. "In the pre-computer age," Alito explained, "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."[322] Only an important investigation would have used such means.[323] GPS devices, however, have made "long-term monitoring relatively easy and cheap."[324] Short-term monitoring using the chips might be one thing, "But the use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy."[325] For those offenses, society did not reasonably expect that law enforcement would "secretly monitor and catalogue every single movement of an individual's car for a very long period."[326] Four weeks was too long.

---

317. *Id.* at 959 (citing Silverman v. United States, 365 U.S. 505, 509 (1961)).

318. *Id.* at 959–60 (citing Rakas v. Illinois, 439 U.S. 128, 143 (1978); Katz v. United States, 389 U.S. 347, 353 (1967) (finding the trespass theory "no longer controlling")).

319. *Id.* at 958.

320. *Id.* at 964.

321. *Id.* at 963.

322. *Jones*, 132 S. Ct. at 963 (Alito, J., concurring).

323. *Id.* at 963–64.

324. *Id.* at 964.

325. *Id.*

326. *Id.*

Justice Sotomayor, in a separate concurrence, agreed.[327] As technology advances, the government will have greater access to geolocational data.[328] In contrast to Scalia, Sotomayor argued that longer-term monitoring impinges on expectations of privacy.[329] Location tracking implicates other rights as well, chilling associational and expressive freedoms.[330] "[T]he Government's unrestrained power to assemble data that reveal private aspects of identity," moreover, "is susceptible to abuse."[331] The privacy interests at stake were considerable. People did not "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."[332] Such a tool, in the hands of the Executive and without any oversight, would be ripe for abuse.[333]

While the majority decided the case on grounds of trespass, what has come to be understood as the shadow majority in *Jones* (the five Justices joining the Alito and Sotomayor concurrences), like the dissents in *Olmstead* and *Goldman*, and the Court in *Silverman*, signaled a growing concern about the impact of new technology on privacy interests protected under the Fourth Amendment.[334]

---

327. *See id.* at 955 (Sotomayor, J., concurring).

328. *See Jones*, 132 S. Ct. at 955 (Sotomayor, J., concurring).

329. *Id.* at 955.

330. *Id.* at 955–56.

331. *Id.* at 956.

332. *Id.*

333. *Id.*

334. The Court has not limited the private/public distinction to land. In 1927 *United States v. Lee* considered the use of a searchlight that uncovered cases of liquor on a boat. 274 U.S. 559, 562–63 (1927). The Supreme Court determined:

> [N]o search on the high seas is shown. The testimony of the boatswain shows that he used a searchlight. It is not shown that there was any exploration below decks or under hatches. For aught that appears, the cases of liquor were on deck and, like the defendants, were discovered before the motorboat was boarded. Such use of a searchlight is comparable to the use of a marine glass or field glass. It is not prohibited by the Constitution.

Id. at 563. Justice Brandeis, writing for the Court, was careful to note that the cases of liquor were simply sitting on the deck and not located below, so no actual entry had to occur for the officers to ascertain that the vessel was carrying contraband. *Id.* Following *Katz*, the private/public distinction persisted for searches conducted on the high seas. Like the location of the buildings on the Dow Chemical's campus, the location of a vessel in the ocean did not "provide the setting for those intimate activities that the [Fourth] Amendment is intended to shelter from government interference or surveillance." Oliver v. United States, 466 U.S. 170, 179 (1984); *see also* Jason R. Crance & Mike Mastry, *Fourth Amendment Privacy Rights at*

E. Enhanced Detection

Starting in the early 1990s, new technologies and techniques that enhanced the human senses, such as thermal imaging, or the use of narcotics dogs, began to make their way onto the Court's docket. Despite the movement in *Katz* to determining privacy from the perspective of the individual (rather than the specific places being protected), the Court continued to rely upon the territorial private/public distinction, with the line drawn at the curtilage of the home.

In 1991, for instance, an agent from the U.S. Department of the Interior suspected that an Oregon resident, Danny Kyllo, was growing marijuana in his home.[335] Knowing that successfully growing the plant indoors required the use of high intensity lamps, the

---

Sea and Governmental Use of Vessel Monitoring Systems: There's Something Fishy About This, 22 J. ENVTL. L. & LITIG. 231, 246 (2007). Arguments regarding the navigation of a vessel paralleled the doctrinal approach to observing a car as it traversed public thoroughfares. *See* United States v. Knotts, 460 U.S. 276, 281 (1983) (quoting Cardwell v. Lewis, 417 U.S. 583, 590 (1974) (Cars have "little capacity for escaping public scrutiny" when traveling on "public thoroughfares where both its occupants and its contents are in plain view.")). Just as the public could observe a car, so, too, could citizens see boats and ships on the open water. Combined with the nature of commercial fishing, a lower expectation of privacy held. Why should government regulators or law enforcement officers be subject to different standards?

Like radio-frequency-enabled transmitters, vessel monitoring systems (VMS) do not provide information located within the vessel, or below deck—making a Fourth Amendment search claim, under the current doctrine, somewhat questionable. Lower courts are divided on whether, and under what circumstances, a captain of a vessel has a reasonable expectation of privacy in what occurs on different parts of the vessel. Crance & Mastry, *supra*, at 247–48. The Fifth Circuit has adopted an approach that mirrors the distinction between open fields and matters located within the curtilage of the home. Since the Coast Guard can conduct administrative inspections of public areas without probable cause and a warrant, the captain of a vessel has no reasonable expectation of privacy in the public areas of the vessel. *See id.* at 247. In *United States v. Freeman*, the Coast Guard located the vessel by means of radar, after which it found more than 41,000 pounds of marijuana on board. 660 F.2d 1030, 1031–34 (5th Cir. 1981), *discussed in* Crance & Mastry, *supra*, at 247. In contrast to the Fifth Circuit, the First Circuit considers that the captain has a reasonable expectation of privacy to the extent that it "derives from his custodial responsibility for the ship, his associated legal power to exclude interlopers from unauthorized entry . . . and the doctrines of admiralty, which grant the captain (as well as the owner) a legal identity of interest with the vessel." United States v. Cardona-Sandoval, 6 F.3d 15, 21 (1st Cir. 1993), *quoted in* Crance & Mastry, *supra*, at 247–48. For non-public areas of the vessel, the circuits agree that those on board do have a reasonable expectation of privacy. *See, e.g.*, United States v. DeWeese, 632 F.2d 1267 (5th Cir. 1980), *cited in* Crance & Mastry, *supra*, at 248.

335. Kyllo v. United States, 533 U.S. 27, 29 (2001).

agent directed a thermal scanner at Kyllo's triplex to detect the level of infrared radiation emanating from the structure.[336] The scan showed a hot spot along the roof over the garage.[337] Based on the results of the test, tips from informants, and Kyllo's utility bills, a federal magistrate judge issued a warrant for a search that yielded 100 marijuana plants.[338]

Justice Scalia, writing for the Court, relied on the walls of the home and the degree to which the observer's senses had been enhanced beyond normal human abilities, to extend Fourth Amendment protections to thermal searches. "The present case," he wrote, "involves officers on a public street *engaged in more than naked-eye surveillance* of a home."[339] Scalia acknowledged, "It would be foolish to contend that the degree of privacy secured to citizens by the Fourth Amendment has been entirely unaffected by the advance of technology."[340] Aircraft had exposed the top of peoples' homes to public view—including portions of the curtilage once considered private. Thermal imaging raised the question of whether limits existed on the "power of technology to shrink the realm of guaranteed privacy."[341] Detecting activity inside the home intruded upon a rule in operation since the founding of the country. "Where, as here, the Government uses a device that is not in general public use, to explore details of the home that would previously have been unknowable without physical intrusion, the surveillance is a 'search' and is presumptively unreasonable without a warrant."[342]

In 2013, the Court considered another sensory enhancement: this time, whether the use of canines outside of a home, to detect narcotics inside the structure, amounted to a search.[343] The Court had previously determined that the use of dogs outside of cars, to detect narcotics inside the vehicle, was not a search.[344] In *Florida v. Jardines*, the Miami-Dade Police Department received a tip that Joe-

336. *Id.*

337. *Id.* at 30.

338. *Id.*

339. *Id.* at 33 (emphasis added).

340. *Id.* at 33–34.

341. *Kyllo*, 533 U.S. at 34.

342. *Id.* at 40.

343. Florida v. Jardines, 133 S. Ct. 1409, 1413 (2013).

344. *See* Illinois v. Caballes, 543 U.S. 405, 410 (2005); *see also* United States v. Place, 462 U.S. 696, 707 (1983) (police exposing luggage at airport to drug-sniffing dog was not a search); Donald A. Dripps, *Perspectives on the Fourth Amendment Forty Years Later: Toward the Realization of an Inclusive Regulatory Model*, 100 MINN. L. REV. 1885, 1906–07 (2016) (discussing *Caballes* and *Jardines*).

lis Jardines was growing marijuana in his home.[345] Two police officers, accompanied by a drug-sniffing dog, went up onto Jardines's front porch.[346] On the basis of the dog's positive response, as well as the tip, the police obtained a warrant to search the home and found cannabis.[347]

Justice Scalia, writing for the Court, repeatedly emphasized the territorial nature of the Fourth Amendment. "The officers were gathering information in an area belonging to Jardines and immediately surrounding his house—in the curtilage of the house," he wrote.[348] "[T]hey gathered that information by physically entering and occupying the area."[349] For Scalia, the physical property proved central: "the home is first among equals."[350]

Once establishing the home as "a constitutionally protected area," Scalia turned to whether an "unlicensed physical intrusion" had occurred.[351] The naked eye, again, figured largely: "While law enforcement officers need not 'shield their eyes' when passing by the home 'on public thoroughfares,' an officer's leave to gather information is sharply circumscribed when he steps off those thoroughfares."[352] In *Ciraolo*, there had been no physical intrusion of the property.[353] The fact that the police in *Jardines* had used a trained animal appears to have mattered little, as the effect was the same: it *altered* law enforcement's ability to detect information about a protected area that was not evident from the use of ordinary senses.

In her concurring opinion, Justice Kagan, joined by Justice Ginsburg and Justice Sotomayor, emphasized the extent to which the canine unit had augmented natural human abilities. "Here," she wrote, "police officers came to Joelis Jardines' door with a super-sensitive instrument, which they deployed to detect things inside that they could not perceive unassisted."[354] Not only was the use of a highly-trained dog without a warrant a violation of the Fourth Amendment, but if the officer had used "super-high-powered binoculars" to look through a window, that, too, could fall

345. 133 S. Ct. at 1413.
346. *Id.*
347. *Id.*
348. *Id* at 1414.
349. *Id.*
350. *Id.*
351. *Jardines*, 133 S. Ct. at 1415.
352. *Id.* (quoting California v. Ciraolo, 476 U.S. 207, 213 (1986)) (citation omitted).
353. *Id.*
354. *Id.* at 1418 (Kagan, J., concurring).

outside constitutional requirements.[355] Kagan noted the "firm" and "bright line" that marked "the entrance to the house," emphasizing the private/public distinction.[356]

Even the dissent turned to some extent upon whether the officer's ordinary senses, outside the curtilage of the home, would suffice. Justice Alito, joined by Chief Justice Roberts, Justice Kennedy, and Justice Breyer, criticized the Court for "fail[ing] to mention that, while [one detective] apparently did not personally smell the odor of marijuana coming from the house, another officer who subsequently stood on the front porch . . . did notice that smell and was able to identify it."[357]

F. Technological Challenges to the Private/Public Distinction

Fourth Amendment doctrine has long struggled with how to integrate new technologies into the private/public distinction. Perhaps nowhere are its failings clearer than in the realm of location tracking.[358]

Two elements are now coming together that undermine the traditional divide. First, the proliferation of tracking technologies means that enormous amounts of locational data are being generated, providing detailed pictures of citizens' lives. Second, the private/public distinction in Fourth Amendment doctrine ignores the possibility that the *length of observation,* the *recording of the information,* or the *analysis of data* obtained from the public domain could trigger a new privacy interests.

The basic argument is that if privacy is not implicated at the front end—i.e., the *moment* an individual sees or hears what a person says or does in public, or reads an individual's documents or papers that are in the public domain—then the length of time that the person is placed under observation, whether the government records the information that is being generated, and whether the government later analyzes the data (potentially in combination with other information) does not give rise to any new privacy right. Zero

355. *Id.* (distinguishing the scenario from delivering the mail or distributing campaign flyers).

356. *Id.* at 1419.

357. *Jardines*, 133 S. Ct. at 1421 (Alito, J., dissenting).

358. Various commentators directly challenge the private/public distinction. *See, e.g.*, Sean K. Driscoll, *"The Lady of the House" vs. a Man with a Gun: Applying* Kyllo *to Gun-Scanning Technology*, 62 CATH. U. L. REV. 601, 604–05 (2013) (discussing the Fourth Amendment implications of firearms scanners using Terahertz Imaging Detection).

plus zero is still zero. Actions in public simply are unprotected by the Fourth Amendment.

This approach is deeply problematic. Locational data, collected in bulk, yields deep insight into individuals' lives. Continued reliance on the private/public distinction fails to capture the interests at stake in public monitoring, and in the collection and analysis of locational data.

1. Digital Tracking

The number of ways that new technologies give others the ability to follow individuals is staggering. WiFi and Bluetooth signals; GPS chips; vessel monitoring systems; RFID tags; automated license plate readers; network connection data; international mobile subscriber identity catchers; Internet protocol databases; financial transactions; consumer purchases; closed circuit televisions; remote biometric identification; and unmanned aerial systems provide just some examples.[359] Tracking has become such an intrinsic feature of modern life that many people do not even realize who is tracing their footsteps. Even a brief discussion illustrates the depth of private information that is available.

Special sensors detect WiFi and Bluetooth-enabled devices, such as mobile telephones, electronic tablets, and computers, as individuals move through public space. Industry is capitalizing on this rich source of data. Companies such as LocationGenius, for instance, guarantee "crowd-sourced scoring and analytics for *any* location"—including retail analytics, audience profiles and impressions, on-demand real estate data, and data related to entire cities or counties for use in urban planning, migration, security, and local law enforcement.[360]

LocationGenius generates customer profiles based on data collected by mobile carriers. The company guarantees that the retailer will instantly know where the customer just was, as well as where their next stop is likely to be.[361] It uses cellular network and device data, sensors, beacons, as well as social media data, to populate a

359. Mobile devices, Internet-connected products, and online activity constantly create data, which can be collected not just by the government, but by private companies that can then trace where people go, how long they spend in each location, and who they are with when they do so. *See* Armina Ligaya, *You're Being Followed: New Digital Tracking Technologies Keep Tabs on Your Every Move*, FINANCIAL POST MAGAZINE, May 7, 2014, http://business.financialpost.com/financial-post-magazine/digital-tracking-privacy?__lsa=0f20-ef2c.

360. LOCATIONGENIUS, http://locationgenius.com (last visited Nov. 19, 2016).

361. *Id.*

profiling engine that "plugs into postal code data, behavioural streams, census data, and . . . other in-house and third party sources," providing retailers with customers' household income, ethnicity, gender, educational level, employment, consumer spending, and brand preferences.[362]

LocationGenius is just one example of a burgeoning industry. The 2016 global market in consumer location information is estimated to be worth more than $16 billion.[363] Mobile marketing (the provision of personalized, time- and location-sensitive information to individuals' mobile devices to promote goods and services) has become standard business practice.[364] The number of applications on a smart phone that collect—and sell—data about the user's movements is extraordinary.[365] Facebook, Google, Foursquare, and Twitter are well known for this. But even seemingly innocuous applications, like Android's popular Brightest Flashlight Free, have tracked and sold users' location information without their knowledge.[366]

---

362. *Id.*; *see also* Ivor Tossell, *Using 'Remarkable' Source of Data, Startup Builds Rich Customer Profiles*, THE GLOBE AND MAIL, Jan. 6, 2014, http://www.theglobeandmail.com/report-on-business/small-business/sb-growth/how-a-startup-is-using-location-data-to-build-rich-customer-profiles-for-retailers/article16187925/.

363. *See* Ligaya, *supra* note 359.

364. *See, e.g.*, Lisa Lacy, *Mobile Marketing Trends 2016: 50 Experts on the Future of Apps, Ads & Search*, LINKDEX (Jan. 4, 2016), http://www.momentology.com/9031-mobile-marketing-trends-2016/; William Comcowich, *Geolocation: The Newest Movement in Mobile Marketing and Measurement,* CYBERALERT (Mar. 15, 2014), http://www.cyberalert.com/blog/index.php/geolocation-the-newest-movement-in-mobile-marketing-and-measurement/; Alan Meyer, *Mobile Marketing and Geolocation: Up Your Effectiveness with Location Targeting*, CARNIVAL.IO, http://insights.carnival.io/mobile-marketing-and-geolocation-up-your-effectiveness-with-location-targeting/ (last visited Nov. 19, 2016); Scott Gerber, *14 Mobile Marketing Trends That Will Dominate in 2016*, MASHABLE (Dec. 23, 2015), http://mashable.com/2015/12/23/mobile-marketing-2016/#boz70c3lZiqp.

365. *See, e.g.*, *About Privacy and Location Services for iOS 8 and iOS 9*, APPLE, https://support.apple.com/en-gb/HT203033 (last visited Nov. 19, 2016) (noting that iOS devices allow maps, camera, weather, traffic, and other apps to use information from cellular, WiFi, GPS networks, and Bluetooth, to determine users' location; also explaining that Location Services triggers location-based system services such as Location-Based Apple Ads, Location Based Alerts, and Share My Location); *see also* Sig Ueland, *10 Geolocation Apps for Business*, PRACTICAL ECOMMERCE (May 13, 2011), http://www.practicalecommerce.com/articles/2780-10-Geolocation-Apps-for-Business (describing Google Latitude; Google Maps; Google Buzz; Double Dutch; Neer; Plancast; Glympse; Foursquare; GroupMe; Hashable; Geoloqi; LiquidSpace).

366. Kristin Burnham, *Location Tracking: 6 Social App Settings to Check*, INFORMATIONWEEK (Aug. 26, 2014, 11:30 AM), http://www.informationweek.com/software/social/location-tracking-6-social-app-settings-to-check/d/d-id/1306643.

GPS chips that record locational data also have become integrated into our daily lives. In 1996, the FCC adopted rules (implemented by 2001) that required all mobile telephones to be GPS-enabled to facilitate emergency services.[367] By 2004, even small carriers had to comply.[368] In 2015, the FCC expanded the rule to require mobile telephone providers to build in the capability to locate cell phones indoors, including the height above ground, enabling law enforcement to pinpoint the precise location of a mobile phone inside a home, office building, or other structure.[369] Wireless carriers do not inform users of any way to disable this function.[370] As long as the phone is turned on, service providers can locate the telephone either through hardware built into the device, or through examining where it connects to the cell site network.

When NAVSTAR opened to commercial interests in 2000, the use of GPS expanded beyond mobile telephones to enable such varied services as access to local resources, time synchronization, and air and ground navigation.[371] The technology is now used by airlines, farming, mining, prisons, security companies, hobbyists, and others to program and track people and objects, and to create virtual borders to monitor people, animals, or objects that enter or leave pre-set boundaries.[372]

---

367. Revision of the Comm'n's Rules to Ensure Compatibility with Enhanced 911 Emergency Calling Sys., 11 FCC Rcd. 18676, 18683–84 (1996).

368. 911 Service, 47 C.F.R. § 20.18 (1999); Revision of the Comm'n's Rules to Ensure Compatibility with Enhanced 911 Emergency Calling Systems, CC No. 94–102, FCC 02–210, at ¶ 32 (July 26, 2002) (order to stay).

369. Wireless E911 Location Accuracy Requirements, PS No. 07–114, FCC 15–9, at ¶¶ 3, 6 (Jan. 29, 2015) (fourth report and order).

370. *See E911 Compliance FAQs*, VERIZON WIRELESS, http://www.verizonwireless.com/support/e911-compliance-faqs.

371. *See* Bradford W. Parkinson, *GPS Eyewitness: The Early Years*, GPS World 5, Sept. 9, 1994, pp. 32–45; MICHAEL RUSSELL RIP & JAMES M. HASIK, THE PRECISION REVOLUTION: GPS AND THE FUTURE OF AERIAL WARFARE, 429–41 (2002); NATIONAL RESEARCH COUNCIL, THE GLOBAL POSITIONING SYSTEM—A SHARED NATIONAL ASSET: RECOMMENDATIONS FOR TECHNICAL IMPROVEMENTS AND ENHANCEMENTS (1995); Eva Marie Dowdell, *Note, You Are Here! – Mapping the Boundaries of the Fourth Amendment with GPS Technology*, 32 RUTGERS COMPUTER & TECH. L. J. 109, 109–10 (2005–2006) (noting the use of GPS for cellular telephony, access to local resources, time synchronization, emergency services, and navigation); KPMG, *Self-driving Cars: The Next Revolution* 34, https://www.kpmg.com/US/en/IssuesAndInsights/ArticlesPublications/Documents/self-driving-cars-next-revolution.pdf.

372. *HTG Explains: What Geofencing Is (and Why You Should be Using It)*, HOW-TO-GEEK, http://www.howtogeek.com/221077/htg-explains-what-geofencing-is-and-why-you-should-be-using-it/ (last visited Oct. 17, 2016); Lauren Brousell, *5 Things You Need to Know About Geofencing*, CIO (Aug. 28, 2013), http://www.cio.com/article/2383123/mobile/5-things-you-need-to-know-about-geofenc-

Vessel Monitoring Systems (VMS) consist of electronic devices that transmit the location of vessels via satellite link to a land-based receiver.[373] The Magnuson-Stevens Fishery Conservation and Management Reauthorization Act of 2006 required that the government increase VMS data sharing among state and federal agencies.[374] On August 9, 2006, the National Marine Fisheries Service published a regulation requiring that *all* vessel owners operating in the Gulf of Mexico outfit their vessels with a VMS unit.[375] The devices must remain on and able to transmit twenty-four hours a day, regardless of where the vessel is located and irrespective of whether the vessel is engaged in commercial fishing. Although supported by environmentalists, the constitutional implications of increased use of VMS mostly have gone unnoticed.[376]

Radio frequency identification (RFID) tags have become more ubiquitous and sophisticated than the beepers used in the investiga-

---

ing.html; *Creating and Monitoring Geofences*, ANDROID DEVELOPERS, http://developer.android.com/training/location/geofencing.html (last visited Oct. 17, 2016); *Geo-fencing*, WHATIS.COM, http://whatis.techtarget.com/definition/geofencing (last visited Oct. 17, 2016); *Geofencing*, TECHOPEDIA, https://www.techopedia.com/definition/14937/geofencing (last visited Oct. 17, 2016). Because of the detail that GPS provides, from its inception, it has been accompanied by significant privacy concerns. *See, e.g.*, David Uris, *Big Brother and a Little Black Box: The Effect of Scientific Evidence on Privacy Rights*, 42 SANTA CLARA L. REV. 995, 1006 (2002) ("[S]keptics can only hope that these devices do not turn out to be Pandora's boxes, for 'the loss of personal civil liberties always begins with the best intentions of the government.'") (citing Bob Van Voris, *Black Box Car Idea Opens Can of Worms,* NAT'L L. J., June 14, 1999, at A1); Simon Romero, *Location Devices' Use Rises, Prompting Privacy Concerns*, N.Y. TIMES, Mar. 4, 2001, http://www.nytimes.com/2001/03/04/business/location-devices-use-rises-prompting-privacy-concerns.html; Petition of the Cellular Telecommunications Industry Association for a Rulemaking to Establish Fair Location Information Practices at 4–5, *In re* Petition for Rulemaking, Nov. 22, 2000; Aaron Reneger, Note, *Satellite Tracking and the Right to Privacy*, 53 HASTINGS L. J. 549 (2002). *See also* Megha Rjagopalan, *Cellphone Companies Will Share Your Location Data – Just Not with You,* PRO PUBLICA (June 26, 2012), https://www.propublica.org/article/cellphone-companies-will-share-your-location-data-just-not-with-you.

373. *Vessel Monitoring System Program—Gulf of Mexico Commercial Reef Fish Frequently Asked Questions*, NATIONAL MARINE FISHERIES SERV., (Apr. 2007), http://sero.nmfs.noaa.gov/sustainable_fisheries/faqs/documents/pdfs/gulf_of_mexico/reef_fish/2012/vms_faqs_041707.pdf; *see also* Crance & Mastry, *supra* note 334, at 233.

374. Magnuson-Stevens Fishery Conservation and Management Reauthorization Act of 2006, Pub. L. No. 109-479, 120 Stat. 3575 (codified as amended at 16 U.S.C. §§ 1801-1883).

375. Fisheries Amendment 18A, 71 Fed. Reg. 45,428 (Aug. 9, 2006) (codified at 50 C.F.R. §§ 622, 635).

376. *But see* Crance & Mastry, *supra* note 334, at 233–34.

tions in *Knotts* and *Karo*.[377] As small as a grain of rice, they can be used to track goods,[378] persons,[379] or animals;[380] to collect tolls;[381] to read travel documents;[382] to verify the authenticity of items;[383] to time sporting events;[384] or to regulate entry into buildings.[385] Enti-

377. A two-way radio with a microprocessor, the device sends out data that is picked up by electronic readers or antennas, to identify the location of people, cars, or objects. Battery-powered RFID chips can typically be read from a range of 300 feet (100 meters) away. *RFID Frequently Asked Questions*, RFID JOURNAL, https://www.rfidjournal.com/faq/show?139.

378. *See, e.g.,* Jill Gambon, *How to Select the Right RFID Tag*, RFID JOURNAL (Oct. 15, 2007), https://www.rfidjournal.com/purchase-access?type=Article&id=3622&r=%2Farticles%2Fview%3F3622; Claire Swedberg, *Meggitt Polymers & Composites Uses RFID to Track Airline Components, Materials*, RFID JOURNAL (Sept. 16, 2016), http://www.rfidjournal.com/articles/view?14984 (reporting that MPC's manufacturing plant is using RFID to track its materials during manufacturing).

379. *See, e.g.,* Sam Witt, *Is Human Chip Implant Wave of the Future?*, CNN, Jan. 14, 1999, available at http://www.cnn.com/TECH/computing/9901/14/chipman.idg/; Rory Cellan-Jones, *Office Puts Chips Under Staff's Skin*, BBC NEWS (Jan. 29, 2015), http://www.bbc.com/news/technology-31042477; John Brandon, *Is There a Microchip Implant in Your Future?*, FOX NEWS (Aug. 30, 2014), http://www.foxnews.com/tech/2014/08/30/is-there-microchip-implant-in-your-future.html. The FDA has issued guidance for the implantation of RFID chips in humans. *Guidance for Industry and FDA Staff—Class II Special Controls Guidance Document: Implantable Radiofrequency Transponder System for Patient Identification and Health Information*, U.S. FOOD AND DRUG ADMIN. CENTER FOR DEVICES AND RADIOLOGICAL HEALTH (Dec. 10, 2014), http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm072141.htm. Companies sell RFID chips to be embedded in human beings for a range of purposes. *See* Dangerous things, RFID & NFC Transponder Implants, available at https://dangerousthings.com/transponders/. When placed under the skin, they can be used to hack phones or to spread computer viruses. *See, e.g.,* Rose Eveleth, *The Man Who Hacks Phones with an Implant Under his Skin*, BBC, May 15, 2017, available at http://www.bbc.com/future/story/20150515-i-hack-phones-with-touch-alone; Mark Gasson, *Human Enhancement: Could you become infected with a computer virus?,* 2010 IEEE International Symposium on Technology and Society, available at http://ieeexplore.ieee.org/document/5514651/.

380. Claire Swedberg, *RFID Goes to the Dogs*, RFID JOURNAL (Aug. 6, 2009) http://www.rfidjournal.com/articles/view?5108.

381. Laurie Wiegler, *Taking a Toll: How RFID is Directing Traffic*, RFID INSIDER (Mar. 6, 2014), http://blog.atlasrfidstore.com/taking-toll-rfid; Claire Swedberg, *RFID Drives Highway Traffic Reports*, RFID JOURNAL (Nov. 16, 2004), http://www.rfidjournal.com/articles/view?1243.

382. Paul Prince, *United States Sets Date for E-Passports*, RFID JOURNAL (Oct. 25, 2006), http://www.rfidjournal.com/articles/view?1951.

383. Claire Swedberg, *RFID Gives Sports Memorabilia Stamp of Authenticity*, RFID JOURNAL (Dec. 21, 2007), http://www.rfidjournal.com/articles/view?3828.

384. Fred O'Connor, *RFID Helps the Boston Marathon Run*, WASH. POST, Apr. 9, 2007, http://www.washingtonpost.com/wp-dyn/content/article/2007/04/09/AR2007040901011.html; Claire Swedberg, *New York City Marathon Offers Enhanced*

ties as disparate as Wal-Mart[386] and the Department of Defense[387] require that vendors use RFID tags to ensure more efficient supply chain management. In 2015, the global RFID market was worth just over $10 billion.[388] By 2020, the market is expected to exceed $13 billion.[389]

Automated license plate readers (ALPRs) pair fixed, portable, and mobile cameras with searchable databases.[390] The small, high-speed cameras, which can capture thousands of car license plates per minute, can be mounted on police cars or city vehicles, as well as stationary objects, such as signs, tollbooths, or bridges. They record the license plate, as well as the date, time, and location of each car. The information is then fed into a local, state, or regional database, with differing levels of retention, depending upon the state.[391]

Network-based data also yields locational data. Service providers record where users' mobile devices connect to local towers—and not just when a telephone call is made or a text message is

RFID-enabled Apps, RFID J., July 25, 2011, http://www.rfidjournal.com/articles/view?8626.

385. *Smart Card Technology FAQ*, SMART CARD ALLIANCE, http://www.smartcardalliance.org/smart-cards-faq/.

386. University Alliance, *RFID Technology Boosts Walmart's Supply Chain Management*, UNIV. OF S.F., http://www.usanfranonline.com/resources/supply-chain-management/rfid-technology-boosts-walmarts-supply-chain-management/#.Vs3L-VKqdfQ (last visited Oct. 17, 2016).

387. *See* Samuel Greengard, *Re-Evaluating Supply Chain Relationships* (Sept. 15, 2014), https://www.rfidjournal.com/purchase-access?type=Article&id=12175&r=%2Farticles%2Fview%3F12175.

388. Raghu Das and Peter Harrop, *RFID Forecasts, Players and Opportunities 2016-2026*, IDTECHEX (Oct. 2015), http://www.idtechex.com/research/reports/rfid-forecasts-players-and-opportunities-2016-2026-000451.asp.

389. *Id.*

390. KIETH GIERLACK, ET AL., LICENSE PLATE READERS FOR LAW ENFORCEMENT 2 (2014), http://www.rand.org/pubs/research_reports/RR467.html.

391. *Automated License Plate Recognition*, INT'L ASS'N OF CHIEFS OF POLICE, http://www.iacp.org/ALPR-FAQs; AM. CIVIL LIBERTIES UNION, YOU ARE BEING TRACKED: HOW LICENSE PLATE READERS ARE BEING USED TO RECORD AMERICANS' MOVEMENTS 18 (July 2013), https://www.aclu.org/feature/you-are-being-tracked. For differing lengths of retention compare Ark. Code (2013) §12-12-1801 to 12-12-1805 (prohibiting data retention beyond 150 days), Cal. Veh. Code (2011) §2413 (prohibiting the California Highway Patrol from retaining data from a license plate reader more than 60 days, unless the information is to be used as evidence in a felony case), Maine (2009), 29-AMRSA §2117-A(2) (setting a 21-day limit on the retention of data obtained via ALPRs), and Tenn. Code (2014) §55-10-302 (putting a 90 day limit on data retention unless the information is part of an ongoing investigation).

received, but constantly, as the user moves through space.[392] The information provides a picture of where individuals go.[393] The courts that have confronted the question of historical cell site location information (CSLI) have struggled with—and split over—whether or not such information is protected.[394] In 2015, the Fourth Circuit held that "the government conducts a search . . . when it obtains and inspects a cell phone user's historical CSLI for an extended period of time."[395] When the case went *en banc,* however, the court reversed its decision.[396] *Smith* controlled. The Eleventh Circuit similarly argued that by using a telephone, mobile users voluntarily provide "location information to telephone com-

392. Patrick DiJusto, *What the N.S.A. Wants to Know About Your Phone Calls*, THE NEW YORKER, June 7, 2013, http://www.newyorker.com/tech/elements/what-the-n-s-a-wants-to-know-about-your-phone-calls.

393. *See* Stephanie K. Pell & Christopher Soghoian, *Can You See Me Now?: Toward Reasonable Standards for Law Enforcement Access to Location Data That Congress Could Enact,* 27 BERKELEY TECH. L. J. 117, 126-27, 168 (2012).

394. Law enforcement has tried to use the Stored Communications Act, as well as the Electronic Communications Privacy Act, to obtain this information. Appellants' Brief, *supra* note 274, at 65. A number of courts, looking to the private nature of the information, the ex parte nature of the proceedings, and the reduced resources required, have required that law enforcement first demonstrate probable cause of a particular crime. *See* Appellants' Brief, *supra* note 274, at 66 (citing *In re* United States for an Order Directing Provider of Elec. Commun. Serv. To Disclose Records to the Gov't, 534 F. Supp. 2d 585, 586–87 (W.D. Pa. 2008)); *In re* Application of the United States of America for an Order Authorizing the Installation and Use of a Pen Register Device, a Trap and Trace Device, and for Geographic Location Information, 497 F. Supp. 2d 301, 302 (D.P.R. 2007); *In re* the Application of the United States of America for an Order Authorizing the Disclosure of Prospective Cell Site Information, 2006 U.S. Dist. LEXIS 73324, at 18, 22 (E.D. Wis. Oct. 6, 2006); *In re* Application of the United States for an Order Authorizing (1) Installation and Use of a Pen Register and Trap and Trace Device or Process, (2) Access to Customer Records, and (3) Cell Phone Tracking, 441 F. Supp. 2d 816, 818–19 (S.D. Tex. 2006); *In re* United States for an Order for Prospective Cell Site Location Info. on a Certain Cellular Tel., No. 06 CRIM. MISC.01, 2006 WL 468300 (S.D.N.Y. Feb. 28, 2006); *In re* United States for Orders Authorizing Installation & Use of Pen Registers & Caller Identification Devices on Tel. Nos., 416 F. Supp. 2d 390, 392 (D. Md. 2006); *In re* the Applications of the United States of America for Order Authorizing the Disclosure of Cell Site Information, 2005 U.S. Dist. LEXIS 43736 (D.D.C. Oct. 26, 2005); *In re* the Application of the United States for an Order Authorizing the Release of Prospective Cell Site Information, 407 F. Supp. 2d 132 (D.D.C. 2005).

395. United States v. Graham, 796 F.3d 332, 344–45 (4th Cir. 2015), *reh'g en banc granted*, 624 F. App'x 75 (4th Cir. 2015).

396. United States v. Graham, No. 12-4659 at *5, (4th Cir. May 31, 2016) (Hein Online).

panies," removing collection of that data by law enforcement from Fourth Amendment protections.[397]

Myriad other ways of obtaining locational data exist. Cell-site simulators, known as "IMSI catchers," can be used to locate mobile telephones within a particular area.[398] The devices essentially pretend to be local cell towers used by mobile service providers, forcing all telephones in a given area that subscribe to the service to issue signals that can be used to locate all phones in the area.[399] The location of an aircard—i.e., a cellular modem that attaches to a computer through the USB port to provide Internet access via a cellular network—can be obtained through similar means.[400] Law enforcement is increasingly turning to IMSI catchers to search for individuals both inside buildings (including homes), as well as in public.[401]

Individuals also can be tracked through databases that map IP addresses to geographic locations.[402] Financial transactions and credit card information can be used to place individuals at a particular location at a particular time.[403] Video cameras, enabled with remote biometric identification, can track individuals as they move through public space.[404] Not only are there more of them, but the

397. United States v. Davis, 785 F.3d 498, 512 n. 12 (11th Cir. 2015).

398. *See* Maryland v. Andrews, 134 A.3d 324, 345 (2016) (holding that the police violated defendant's reasonable expectation of privacy under the 4th Amendment by using real-time cell phone information to find the precise location of an individual within a home); *see also* Dan Goodhin, *Low-cost IMSI Catcher for 4G/LTE Networks Tracks Phones' Precise Locations*, ARS TECHNICA (Oct. 28, 2015), http://arstechnica.com/security/2015/10/low-cost-imsi-catcher-for-4glte-networks-track-phones-precise-locations/; *Stingray Tracking Devices: Who's Got Them?*, ACLU, https://www.aclu.org/map/stingray-tracking-devices-whos-got-them (last visited Oct. 16, 2016). Note that "Stingray," made by Harris Corporation, is one of the most well-known IMSI catchers, but there are various other models on the market.

399. Brief for Electronic Frontier Foundation, et al. as Amici Curiae Supporting Defendant-Appellant at 19, United States v. Patrick, No. 15-2443 (7th Cir. Jan. 22, 2016).

400. *See, e.g.*, 844 F. Supp. 2d 982, 987 (D. Ariz. 2013).

401. *See, e.g.*, United States v. Patrick, No. 13-CR-234, 2015 WL 106158, at *2–*3 (data from carrier used to identify general location of a telephone, with an IMSI catcher, then employed to pinpoint the precise location of the telephone within an apartment), argued, No. 15-02443 (7th Cir. May 24, 2016).

402. *See, e.g.*, *What Is Geolocation of an IP Address?*, IP LOCATION FINDER, www.iplocation.net.

403. *See, e.g.*, *Privacy & Credit Card Records: What Does Your Online & Credit History Reveal?*, CYBER TREND (Apr. 8, 2015), http://www.cybertrend.com/article/17089/privacy-and-credit-card-records.

404. *See, e.g.*, ISACA, GEOLOCATION: RISK, ISSUES AND STRATEGIES 5, 8 (2011), http://www.isaca.org/groups/professional-english/wireless/groupdocuments/geolocation_wp.pdf; Andrew E. Taslitz, *The Fourth Amendment in the Twenty-First Cen-*

technologies involved in storing, analyzing, and combining the data with other sources is steadily "growing exponentially more powerful."[405] Even kinetic photos taken by a smart phone include location data and time and date stamps (when these functions are not disabled). Images can be read using facial recognition technology, placing particular individuals in particular places at particular times.

When cameras are mounted on unmanned aerial systems (UAS), mobile monitoring may be enabled.[406] Drones open new ways to conduct surveillance.[407] They can fly virtually undetected at higher altitudes, remain stationary outside buildings at lower altitudes, and follow individuals in real time.[408] They can be programmed to track GPS chips and can be fitted with video and audio surveillance equipment, with the information continuously recorded either on the device or at a remote location.[409] Drones can incorporate technologies ranging from remote biometric identification and heat sensors, to radar, infrared cameras, and "sniffers," enabling them to detect particles suspended in the air.[410] Although

---

tury: Technology, Privacy, and Human Emotions, 65 LAW & CONTEMP. PROBLEMS 125, 127 (2002) (discussing Tampa, Florida law enforcement pairing of CCTV and facial recognition technology to find criminals in crowds).

405. David Alan Sklansky, *Too Much Information: How Not to Think About Privacy and the Fourth Amendment*, 102 CAL. L. REV. 1069, 1085–86 (2014).

406. Andrew Conte, *Drones with Facial Recognition Technology Will End Anonymity, Everywhere*, BUSINESS INSIDER (May 27, 2013), http://www.businessinsider.com/facial-recognition-technology-and-drones-2013-5.

407. Over the past five years, there has been an upsurge in the number of law review notes, comments, and articles looking at the impact of drones on Fourth Amendment doctrine. *See, e.g.*, M. Ryan Calo, *The Drone as Privacy Catalyst,* 64 STAN. L. REV. ONLINE 29, 32 (2011); Matthew R. Koerner, Note*, Drones and the Fourth Amendment: Redefining Expectations of Privacy*, 64 DUKE L. J. 1129 (2015); Timothy T. Takehashi, *Drones and Privacy*, 14 COLUM. SCI. & TECH. L. REV. 72, 72 (2013); Andrew B. Talai, Comment*, Drones and* Jones: *The Fourth Amendment and Police Discretion in the Digital Age*, 102 CAL. L. REV. 729, 731–32 (2014); John Villasenor, *Observations from Above: Unmanned Aircraft Systems and Privacy,* 36 HARV. J. L. & PUB. POL'Y 457, 459 (2013); Philip J. Hiltner, Comment, *The Drones Are Coming: Use of Unmanned Aerial Vehicles for Police Surveillance and Its Fourth Amendment Implications,* 3 WAKE FOREST J. L. & POL'Y 397, 397 (2013).

408. *See also* Koerner, *supra* note 407, at 1133, 1150–53 (noting the unique qualities of drones and the range of technologies that they carry).

409. *See also* ANUJ PURI, A SURVEY OF UNMANNED AERIAL VEHICLES (UAV) FOR TRAFFIC SURVEILLANCE 1, 2 (2005) (unpublished manuscript), http://www.ugpti.org/smartse/research/citations/downloads/Puri-A_Survey_of_Unmanned_Aerial_Vehicles_for_Traffic_Surveillance-2005.pdf.

410. Andrew Conte, *supra* note 406; *Surveillance Drones*, ELECTRONIC FRONTIER FOUNDATION, https://www.eff.org/issues/surveillance-drones. *See also Surveillance and Monitoring with UAVs*, MICRODRONES.COM, https://www.microdrones.com/en/

the battery time for most commercial drones is limited (up to 90 minutes in the air),[411] custom builds can be designed to stay aloft longer, with replacements sequenced to provide for continuous surveillance.[412] Not only are drones more maneuverable and in many ways more technologically sophisticated than helicopters, but they also require fewer resources to operate. While a police helicopter may cost upwards of one million dollars just for the aircraft (not to mention fuel, pilots, and other equipment), drones run in the tens to hundreds of dollars.[413]

Together, these and other technologies enable industry and government to collect massive amounts of information about individuals as they move through public space.[414] Four points here deserve notice.

First, it appears that law enforcement is making increasing use of locational information. For example, according to RAND, by 2014, 71% of state police departments were using license plate readers, while 85% of police departments stated that they planned to obtain or to expand their use of the technology.[415] Vermont's statewide ALPR system yielded nearly nine million records between July 2013 and December 2014.[416] The Northern California Regional Intelligence Center, which covers the area from Monterey County up to Humboldt County, collected more than forty-six mil-

applications/areas-of-application/monitoring/ (noting use of "a thermal camera payload so that living beings . . . can be more easily detected in darkness or in dense vegetation," and listing the range of surveillance activities that the drone can undertake).

411. *See* Korey Smith, *General Drone Specs and Price Chart*, MyFirstDrone.com (Oct. 1, 2016), http://myfirstdrone.com/tutorials/buying-guides/best-drones-for-sale/; *Microdrones MD4-1000: Robus and Powerful UAV/Drone Model*, Microdrones, https://www.microdrones.com/en/products/md4-1000/at-a-glance/ (last visited Oct. 17, 2016).

412. Military drones can stay aloft for hours or days at a time, with coverage of entire cities, as well as the ability to read a milk carton from 60,000 feet in the air. *Surveillance Drones*, Electronic Frontier Foundation, https://www.eff.org/issues/surveillance-drones (last visited Oct. 17, 2016).

413. Koerner, *supra* note 407, at 1148–49.

414. Transit passes, access cards, and automated toll booth systems provide just a few of many more examples of location tracking.

415. Keith Gierlack, et al., *License Plate Readers for Law Enforcement: Opportunities and Obstacles,* RAND Corporation (2014), at 8, http://www.rand.org/pubs/research_reports/RR467.html.

416. VT Dep't Pub. Safety, Annual Report to the Vermont Senate and House Committees on Judiciary and Transportation as Required by 23 V.S.A. §1607, Automated License Plate Recognition Systems (2015), http://mediad.publicbroadcasting.net/p/vpr/files/201503/VT-2014-ALPR-Annual-Report-VPR.pdf.

lion images between May 2014 and April 2015.[417] The impact of even a single officer using a license reader is significant: one policeman in Maryland was able to scan more than 48,000 vehicles over a 27-day period, in the process issuing 255 traffic citations and finding 26 drivers with suspended licenses, 16 vehicle-emission violations, 4 stolen cars, and 1 expired license plate.[418]

Private industry has moved into the ALPR field. Digital Recognition Network, for instance, claims to scan 40% of all U.S. vehicles each year.[419] They operate in conjunction with approximately 400 car repossession companies across the country, scanning up to 1800 plates per minute.[420] The involvement of private industry has, in turn, generated more government use of the technology. Vigilant states that its ALPR database includes more than 2.8 billion plate scans, which it expands by more than seventy million scans per month.[421] It provides the system for free to Texas law enforcement.[422] In return, the government gives Vigilant access to outstanding court fees, which the company links to the license plates of those owing the fees.[423] It then alerts law enforcement when the cars are found, giving officers the opportunity to pull over the cars to obtain the fees, along with a 25% processing fee, which is then given directly back to Vigilant.[424] Vigilant's privacy policy notes, "The images stored in the system are collected from areas visible to

417. Samantha Weigel, *Who's Watching Who?: License Plate Readers Used Throughout San Mateo County,* THE DAILY JOURNAL (Apr. 8, 2015), http://www.smdailyjournal.com/articles/lnews/2015-04-08/whos-watching-who-license-plate-readers-used-throughout-san-mateo-county/1776425141346.html; *see also* NCRIC ALPR FAQs, NORTHERN CALIFORNIA REGIONAL INTELLIGENCE CENTER (Feb. 2015), https://ncric.org/html/ALPR-FAQ-Feb-2015.pdf.

418. Jeremy Hsu, *70 Percent of U.S. Police Departments Use License Plate Readers*, IEEE SPECTRUM (Jul. 8, 2014), http://spectrum.ieee.org/cars-that-think/transportation/sensors/privacy-concerns-grow-as-us-police-departments-turn-to-license-plate-readers; Weigel, *supra* note 417 (noting that one patrol car, with four mounted ALPRs, can obtain some 10,000 images during a 12-hour shift).

419. Seth Wenig, *Private License Plate Scanners Amassing Vast Databases Open to Highest Bidders*, RT (Mar. 6, 2014), https://www.rt.com/usa/license-scanners-private-database-046/.

420. *Id.*

421. Dave Maass, *"No Cost" License Plate Readers Are Turning Texas Police into Mobile Debt Collectors and Data Miners*, ELECTRONIC FRONTIER FOUNDATION (Jan. 26, 2016), https://www.eff.org/deeplinks/2016/01/no-cost-license-plate-readers-are-turning-texas-police-mobile-debt-collectors-and; *see also*, *Vigilant Products*, VIGILANT SOLUTIONS, https://vigilantsolutions.com/products (last visited Oct. 17, 2016).

422. Maass, *supra* note 421.

423. *Id.*

424. *Id.*

the public where there is no reasonable expectation of privacy."[425] The company further claims a First Amendment right to collect and disseminate the information.[426] Vigilant retains the right to sell the data to anyone for commercial purposes, as well as for market research purposes.[427] And it retains the information "as long as it has commercial value."[428]

Like companies, individuals also can make use of the technology. Whether in public, commercial, or private hands, the price of the scanners is steadily falling,[429] even as they are subject to few, if any, legal limits.

As for cell site simulators, the ACLU, has documented sixty-six agencies in two dozen states, as well as Washington, D.C., that own and use them.[430] At the federal level, the FBI; DEA; U.S. Secret Service; Immigration and Customs Enforcement; U.S. Marshals Service; Bureau of Alcohol, Tobacco, Firearms, and Explosives; Internal Revenue Service; U.S. Army; U.S. Navy; U.S. Marine Corps; U.S. National Guard; U.S. Special Operations Command; and National Security Agency all own IMSI catchers.[431]

Network data collected by companies similarly appears to be a growing source of government data. Seven years ago, a Sprint/Nextel executive claimed that over the previous thirteen months, the company had received some eight million requests from law enforcement for location data.[432] In 2012, a Congressional inquiry found that cell phone carriers had provided subscriber information relating to texts, locational data, and calling records, to law enforcement some 1.3 million times.[433]

---

425. *LPR Usage and Privacy Policy*, VIGILANT SOLUTIONS, https://vigilantsolutions.com/lpr-usage-privacy-policy (last visited Oct. 17, 2016).

426. *Id.*

427. *Id.*

428. *Id.*

429. Julia Angwin & Jennifer Valentino-Devries, *New Tracking Frontier: Your License Plates*, WALL ST. J. (Sept. 29. 2012), http://online.wsj.com/article/SB10000872396390443995604578004723603576296.html.

430. *Stingray Tracking Devices: Who's Got Them?*, ACLU, https://www.aclu.org/map/stingray-tracking-devices-whos-got-them (last visited Oct. 17, 2016).

431. *Id.*

432. Herbert, *supra* note 274, at 462 (citing Kevin Bankston, *Surveillance Shocker: Sprint Received 8 Million Law Enforcement Requests for GPS Location Data in the Past Year,* ELECTRONIC FRONTIER FOUNDATION (Dec. 1, 2009, 1:45 PM), http://www.eff.org/deeplinks/2009/12/surveillance-shocker-spring-received-8-million-law).

433. David Kravets, *1.3M Cellphone Snooping Requests Yearly? It's Time for Privacy and Transparency Laws,* WIRED (Jul. 11, 2012), https://www.wired.com/2012/07/mobile-data-transparency/.

As for drones, in 2014, when a rancher refused to turn over six cows that had wandered onto his property, North Dakota law enforcement enlisted the aid of a DHS Predator drone to locate and arrest him.[434] Although the state prosecutor stated that it was the first time unmanned surveillance aircraft had been used by North Dakota, between 2010 and 2012 Customs and Border Patrol had already flown nearly 700 surveillance missions for federal, state, and local law enforcement agencies.[435]

Quite apart from the federal arsenal, Grand Forks County, North Dakota operates its own drones.[436] In 2011, the Sheriff's Department began training a Small Unmanned Aircraft Unit in collaboration with the University of North Dakota's John D. Odegard School of Aerospace Sciences.[437] In March 2013, the FAA explicitly authorized the Sheriff's Department to use drones for law enforcement purposes.[438] The first use of a drone during a police mission was in May 2013.[439] Two years later, North Dakota became the first

434. Joe Wolverton, II, *First Man Arrested by Aid of Drone Convicted in North Dakota,* NEW AMERICAN (Feb. 1, 2014), http://www.thenewamerican.com/usnews/constitution/item/17534-first-man-arrested-by-aid-of-drone-convicted-in-north-dakota. *See also* Jason Koebler, *North Dakota Man Sentenced to Jail in Controversial Drone-Arrest Case*, U.S. NEWS & WORLD REPORT (Jan. 15, 2014), http://www.usnews.com/news/articles/2014/01/15/north-dakota-man-sentenced-to-jail-in-controversial-drone-arrest-case; Michael Peck, *Predator Drone Sends North Dakota Man to Jail*, FORBES (Jan. 27, 2014), http://www.forbes.com/sites/michaelpeck/2014/01/27/predator-drone-sends-north-dakota-man-to-jail/#37c69afd5853.

435. Peck, *supra* note 434; *see also* Jennifer Lynch, *Customs & Border Protection Loaned Predator Drones to Other Agencies 700 Times in Three Years According to "Newly Discovered" Records*, ELECTRONIC FRONTIER FOUNDATION (Jan. 4, 2014), https://www.eff.org/deeplinks/2014/01/newly-discovered-drone-records-show-customs-border-protection-flew-its-predator.

436. Kelsey D. Atherton, *Inside One of the FAA's New Drone Test Sites*, POPULAR SCIENCE (Jan. 2, 2014), http://www.popsci.com/article/technology/inside-one-faas-new-drone-test-sites. In November 2012, the FAA issued Grand Forks county (North Dakota) Sheriff's Department a Certificate of Authorization, permitting the operation of a Draganflyer X6 small unmanned aircraft system (sUAS) in 16 counties in northeastern North Dakota. Press Release, Grand Forks County Sheriff's Department, Small Unmanned Aircraft System (Dec. 6, 2012), http://www.draganfly.com/pdf/Grand%20Forks%20County%20-%20Press%20Release.pdf (explaining that the drone has six rotors, weighs less than three pounds, and streams real-time video to ground station and takes high-definition digital still images).

437. *See* Press Release, *supra* note 436.

438. *See* Atherton, *supra* note 436.

439. *Id.*

state to legalize the use of armed drones, pairing surveillance concerns with non-lethal force.[440]

The number of police departments using drones continues to expand.[441] By 2015, some two dozen had been fully equipped in their use, with sixty more requesting FAA certification.[442] Only fourteen states require a warrant prior to law enforcement using drones for surveillance.[443]

The second observation to be made is that the insight provided by such data into individuals' private lives is profound. Locational tracking shows where you go, what you do, and who you are with when you do so.[444] It can reveal an individual's identity,[445] race,[446]

440. H.R. 1328, 64th Leg. (N.D. 2015) at § 5(1) (only prohibiting the use of unmanned aerial vehicles "armed with any lethal weapons"); *see also* Henry Austin, *North Dakota Becomes First U.S. State to Legalize Use of Armed Drones by Police*, INDEPENDENT (Sept. 8, 2015), http://www.independent.co.uk/news/world/americas/north-dakota-becomes-first-us-state-to-legalise-use-of-armed-drones-by-police-10492397.html; Justin Glawe, *First State Legalizes Taser Drones for Cops, Thanks to a Lobbyist*, THE DAILY BEAST (Aug. 26, 2016), http://www.thedailybeast.com/articles/2015/08/26/first-state-legalizes-armed-drones-for-cops-thanks-to-a-lobbyist.html.

441. Not only do police departments operate their own devices, but private drone footage has also been used in arrests. *See, e.g.*, Jordan Pearson, *Meet the 'Drone Vigilante' Who Spies on Sex Workers,* MOTHERBOARD (Apr. 4, 2016), http://motherboard.vice.com/read/drone-vigilante-brian-bates-johntv-oklahoma-spies-on-sex-workers?trk_source=popular.

442. Veronique Dupont, *Drone Policing in U.S. Seen as "Wild West,"* YAHOO! NEWS (Sept. 12, 2015), https://www.yahoo.com/news/drone-policing-us-seen-wild-west-215907770.html; Anthea Mitchell, *Should America Be Worried About Police Drones?*, THE CHEATSHEET (May 15, 2015), http://www.cheatsheet.com/politics/are-police-drones-a-privacy-nightmare-or-a-safety-advantage.html/?a=viewall; ***see*** *also* 2011-2012 FAA List of Drone License Applicants, obtained via FOIA request, available at https://www.eff.org/document/2012-faa-list-drone-applicants.

443. Kaveh Waddell, *Few Privacy Limitations Exist on How Police Use Drones,* THE ATLANTIC (Feb. 5, 2015), http://www.theatlantic.com/politics/archive/2015/02/few-privacy-limitations-exist-on-how-police-use-drones/458583/.

444. *See generally* Andrew J. Blumberg & Peter Eckersley, *On Locational Privacy, and How to Avoid Losing it Forever*, ELECTRONIC FRONTIER FOUNDATION, 1–2 (Aug. 2009), https://www.eff.org/files/eff-locational-privacy.pdf (discussing how systems have "strip[ped] away" locational privacy by allowing other people to find out personal information by "consulting location databases").

445. A. Cecaj, M. Mamei & N. Bicocchi, The Third IEEE International Workshop on the Impact of Human Mobility in Pervasive Systems and Applications, *Re-Identification of Anonymized CDR Datasets Using Social Network Data*, 237–42 (2014); S. Ji, W. Li, M. Srivatsa, J. S. He, & R. Beyah, *Structure Based Data De-Anonymization of Social Networks and Mobility Traces*, INFORMATION SECURITY 237, 237–54 (2014); A. Cecaj, M. Mamei & F. Zambonelli, *Re-Identification and Information Fusion Between Anonymized CDR and Social Network Data*, J. AMBIENT INTELLIGENCE & HUMANIZED COMPUTING 83, 83 (Jul. 14, 2015); Yves-Alexandre de Montjoye, et al., *Unique in the*

gender,[447] age,[448] marital status,[449] religious beliefs, medical conditions, occupation,[450] and intimate relationships.[451] It records hobbies and predilections. And it can be used to predict where an individual is likely to be and what an individual is likely to do—and with whom—in the future.[452] In 2011, the Information Systems Audit and Control Association (ISACA), a non-profit, multi-national trade organization, noted "a growing consensus that geolocation data should be classified as sensitive."[453] The organization evinced concern that "current law does not articulate a stance on the privacy and security aspect of geolocation."[454] More recently, a team of researchers from Louvain University in Belgium, and Harvard and MIT in the United States, warned that "Given the amount of information that can be inferred from mobility data, as well as the potentially large number of . . . mobility datasets available," significant implications for privacy are on the line.[455]

Crowd: The Privacy Bounds of Human Mobility, NATURE (Mar. 25, 2013), http://www.nature.com/articles/srep01376.

446. Christopher J. Riederer, Sebastian Zimmeck, Coralie Phanord, Augustin Chaintreau & Steven M. Bellovin, *"I Don't Have a Photograph, But You Can Have My Footprints."—Revealing the Demographics of Location Data*, COSN' 15: PROC. 2015 ACM CONF. ON ONLINE SOC. NETWORKS 185, 192 (Nov. 2, 2015).

447. N. J. Yuan, W. Zhong, F. Zhang, & X. Xie, *You Are Where You Go: Inferring Demographic Attributes from Local Check-ins*, WSDM '15: PROC. 8TH ANNUAL ACM INT'L CONF. ON WEB SEARCH AND DATA MINING 295, 297 (2015); Sanja Brdar, Dubravko Culibrk & Vladimir Crnojevic *Demographic Attributes Prediction on the Real-World Mobile Data*, MOBILE DATA CHALLENGE WORKSHOP (2012), https://research.nokia.com/files/public/mdc-final202-brdar.pdf, *cited in* Steven M. Bellovin, Renee M. Hutchins, Tony Jebara & Sebastian Zimmeck, *When Enough Is Enough: Location Tracking, Mosaic Theory, and Machine Learning*, 8 N.Y.U. J. L. & LIBERTY 556, 559 & n.8 (2013–2014).

448. *See* Brdar et al., *supra* note 447.

449. *See* Yuan et. al, *supra* note 447, at 297; *see also* Brdar et al., *supra* note 447.

450. *See* Brdar et al., *supra* note 447.

451. *See generally* E. Cho, S. A. Myers & J. Leskovec, *Friendship and Mobility: User Movement in Location-Based Social Networks*, KDD '11: PROC. 17TH ACM SIGKDD INT'L CONF. ON KNOWLEDGE DISCOVERY & DATA MINING 1082 (2011) (using cell phone data as evidence to advance understanding of the "basic laws governing human movement and dynamics."); David J. Crandall, et al., *Inferring Social Ties from Geographic Coincidences*, 107 PROC. OF THE NAT'L ACAD. OF SCI. 22436 (2010).

452. *See* Riederer, et al., *supra* note 446, at 192; Bellovin, et al., *supra* note 447, at 558 n.9.

453. ISACA, GEOLOCATION: RISK, ISSUES AND STRATEGIES 5, 9 (2011), http://www.isaca.org/groups/professional-english/wireless/groupdocuments/geolocation_wp.pdf.

454. *Id.*

455. *See* Montjoye, et al., *supra* note 445, at 4.

Third, the fact that industry itself is collecting this data has implications for government access to the information. As a matter of law, the Supreme Court in *Kyllo* cited the ubiquitous nature of technology as a consideration in whether individuals held a privacy interest in it. Underlying the legal argument is the same approach that marks the private/public distinction: if private corporations have access to the information, then why should the government be forced to close its eyes or cover its ears? And legal doctrine goes further: since the 1970s, the decision by consumers to entrust this data to third parties means that individuals no longer hold a privacy right in the information (see discussion, *infra* Part IV).[456]

Fourth, to the extent that the Fourth Amendment analysis hinges on an initial determination at the moment of collection, it does not provide for a later interest to arise as the volume of information expands. The basic argument, which Foreign Intelligence Surveillance Court (FISC) Judge Claire Eagan expressed with regard to the NSA collection of telephony metadata under Section 215 of the USA PATRIOT Act, is that zero plus zero still equals zero.[457] If there is no privacy interest at the front end, then increasing the amount of time, or the volume of information, does not bring a privacy interest into being *ex nihilo*.[458]

The problem with applying this approach to the collection of locational data is that the private/public distinction on which it is based fails to acknowledge the additional privacy interests entailed in repeated observation. The value of aggregated information changes when there is more of it.[459]

As the lower courts have confronted the questions raised by these new technologies, a number have eschewed privacy considerations. In 2012, for instance, the Sixth Circuit considered law enforcement's use of subscriber information, cell site information,

456. *See* Paul Ohm, *The Fourth Amendment in a World Without Privacy*, 81 Miss. L. J. 1309, 1331 (2012) (exploring the relationship between public and private surveillance).

457. *In re* Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things from [Redacted Text], BR 13-109, at 9 (FISA Ct. Aug. 29, 2013), https://www.aclu.org/files/assets/br13-09-primary-order.pdf; *see also* Donohue, *Bulk Metadata*, *supra* note 6, at 867 (discussing Judge Eagan's approach); Donohue, Future, *supra* note 6, at 120–21.

458. *See* Donohue, *Bulk Metadata*, *supra* note 6, at 867 (discussing Judge Eagan's approach).

459. Bellovin et al., *supra* note 447, at 558–59. This approach also ignores the important role of limited resources in protecting privacy. Law enforcement only has access to a certain amount of police time. Thus, the placement of a tail on a suspect has to rise to a level of importance that would justify using the resources.

GPS real-time location, and "ping" data to find the location of a drug dealer.[460] The Court considered *Knotts* as controlling.[461]

Judge Rogers began *United States v. Skinner* by stating, "When criminals use modern technological devices to carry out criminal acts and to reduce the possibility of detection, they can hardly complain when the police take advantage of the inherent characteristics of those very devices to catch them."[462] The drug runners had used "pay as you go (and thus presumably more difficult to trace) cell phones to communicate."[463] For the court, Skinner had no "reasonable expectation of privacy in the data given off" by his phone.[464] Collecting the data was akin to "trailing a defendant."[465] That it was more efficient, or effective, did not make it unconstitutional.[466] A few other courts have come to a similar conclusion for historic cell site data.[467]

Not all courts agree. Some state courts have come out on the other side of the question, finding constitutional protections. The Massachusetts Supreme Judicial Court considers mobile phone location data to be even more concerning than the use of GPS for cars, because of the greater privacy interests at stake.[468] The New Jersey Supreme Court similarly has held that cell phone location data, in particular, blurs the distinction between public and private space.[469] The Florida Supreme Court similarly considers the use of cell site location information to constitute a search within the meaning of the Fourth Amendment—thus triggering the need for a prior warrant.[470] The court warned, "the ease with which the government, armed with current and ever-expanding technology, can now monitor and track our cellphones, and thus ourselves, with minimal expenditure of funds and manpower, is just the type of 'gradual and silent encroachment[ ]' into the very details of our

460. United States v. Skinner, 690 F.3d 772, 774 (2012).

461. *Id.* at 777.

462. *Id.* at 774.

463. *Id.*

464. *Id.* at 777.

465. *Id.* at 778.

466. *See* United States v. Forest, 355 F.3d 942, 951 (6th Cir. 2004) (pinging a cell phone to make up for having lost visual contact with a suspect considered outside Fourth Amendment protections because "the DEA agents could have obtained the same information by following the car").

467. *See, e.g.*, United States v. Davis, 785 F.3d 498, 518 (11th Cir. 2015) (en banc), *cert. denied*, 135 S. Ct. 479 (2015) (mem.); *In re* Application for Cell Site Data, 724 F. 3d 600, 600 (5th Cir. 2013).

468. Commonwealth v. Augustine, 4 N.E. 3d 846, 861–62 (Mass. 2014).

469. State v. Earls, 70 A.3d 630, 642 (N.J. 2013).

470. Tracey v. State, 152 So. 3d 504, 526 (Fla. 2014).

lives that we as a society must be vigilant to prevent."[471] Other courts have taken a similar approach for historic cell site data[472] as well as live tracking.[473]

In sum, despite *Katz*'s recognition that the Fourth Amendment protects people, not places, the doctrine has doggedly held on to the property assumptions that marked *Olmstead*. The Supreme Court continues to rely on the curtilage of the home, and the operation of the senses as the litmus test for whether new technologies trigger Fourth Amendment interests at the outset—placing further privacy claims beyond constitutional reach. The Court's logic is that when an individual leaves the protections of the home, anything one says or does can be seen and heard by others. Law enforcement officers, in turn, should not be forced to close their eyes or to cover their ears. They have a right to be in public, and to observe what others witness.

That may be true as far as walking down the street on a particular occasion. But for *all* such movements to be observed, recorded, and analyzed, another individual would have to follow us around twenty-four hours a day, for days, even months or years on end. There are two problems with this claim.

First, what one person could observe at a particular moment can be considered qualitatively different from what one person could observe at all times. There is a distinction to be drawn here between single observation and multiple incident observations. When driving down the street, for instance, it is not just unlikely, but virtually impossible for a bystander to track all of our movements in a car.[474] Another person also could be in a car, tailing us, but as most people who have had to follow a friend just to get to one destination could attest, even on a limited basis, when both drivers *know* that that is the pre-arranged plan *and are trying to do it*,

471. *Id.* at 522 (quoting James Madison, Speech in the Virginia Ratifying Convention on Control of the Military (June 16, 1788)); *see also* Brief for Electronic Frontier Foundation, et al. as Amici Curiae Supporting Defendant-Appellant at 19–20, United States v. Patrick, No. 15-2443 (7th Cir. Jan. 22, 2016).

472. *See, e.g.*, United States v. Graham, 796 F.3d 332, 344–45 (4th Cir. 2015), *reh'g en banc granted*, 624 F. App'x 75 (4th Cir. 2015); *In re* Application for Tel. Info. Needed for a Criminal Investigation, 2015 WL 4594558 at *12 (N.D. Cal. 2015), *appeal dismissed*, No. 15-16760 (9th Cir. 2016).

473. *See, e.g.*, United States v. White, 62 F. Supp. 3d 614, 622–23 (E.D. Mich. 2014); United States v. Powell, 943 F. Supp. 2d 759, 793 (E.D. Mich. 2013).

474. *See* Stephen E. Henderson, *Nothing New Under the Sun? A Technologically Rational Doctrine of Fourth Amendment Search*, 56 MERCER L. REV. 507, 548 (2005) ("[M]ost drivers would not think they were conveying their entire driving route to bystanders.").

tailing can be difficult to put into execution. Lights change. The second car may miss the light. If the first car does not pull over to wait, it can be difficult for the second car to catch them. One car may need to stop at a train junction, or when a school bus stops to let off children. An emergency vehicle may block the road, or a pedestrian may enter a crosswalk. Other cars may cut between the two vehicles, making it difficult to see the lead car. This may cause the second car to miss a turn. One car may have car trouble and have to pull over. Myriad hindrances may arise—even while following one car, for a limited time, to get to one destination. Multiply these factors for every destination over an indefinite period, and the sheer unlikelihood of successfully observing every moment becomes clear. No bystander could collect this kind of information.

Second, no one reasonably expects that another person *would* engage in such behavior. To the contrary, if someone did attempt to monitor one's every move, many people would regard it as not just unacceptable but downright creepy. This is why we have temporary restraining orders.[475] They are used to prevent others from invading our private lives—even if their actions are limited to tracking our every move in the public domain.

2. Recording and Analysis: Informants and the First Amendment

New technologies allow not just for public tracking, but also for the *recording* and *analysis* of the data. These are two separate steps. Yet neither operation triggers protections under the Fourth Amendment—even though the act of recording allows for more information to be obtained, which, when analyzed, yields yet deeper insight into an individual's life.

a. Recording of Data

In *United States v. Caceres*, another case from the 1970s, the Supreme Court considered whether the secret recording of a private conversation by someone privy to the communication qualified as a search within the meaning of the Fourth Amendment.[476] It con-

475. 18 U.S.C. § 2261A (2006) (to obtain a temporary restraining order under federal law, an individual must, *inter alia*, demonstrate the other person's intent to "harass, or place under surveillance with intent to kill, injure, harass, or intimidate another person"); *Domestic Violence Civil Protection Orders (CPOs)*, AM. BAR ASS'N COMM'N ON DOMESTIC & SEXUAL VIOLENCE (Mar. 2014) (listing all state TRO laws, also known as civil protection orders, civil harassment restraining orders, or stalking protective orders), http://www.americanbar.org/content/dam/aba/administrative/domestic_violence1/Resources/statutorysummarycharts/2014%20CPO%20Availability%20Chart.authcheckdam.pdf.

476. 440 U.S. 741 (1979).

cluded that it did not: "Neither the Constitution nor any Act of Congress requires that official approval be secured before conversations are overheard or recorded by Government agents with the consent of one of the conversants."[477] The information merely reproduced what the agent could have written down, so no further privacy interest was implicated.

In its ruling, the Court relied on a series of cases, in which the Court had considered whether the recording of the information altered the quality of the privacy intrusion and concluded that it had not.

The first case in the series was the 1952 case of *On Lee v. United States*, in which an undercover agent, wired with a microphone, was sent into the suspect's laundromat to obtain incriminating evidence.[478] An agent from the Bureau of Narcotics, who listened to the conversations inside the laundromat from a remote location, later testified at trial.[479] Writing on behalf of the Court, Justice Jackson suggested that by allowing the agent onto his premises, and divulging incriminating information, On Lee had consented to law enforcement access to the information.[480]

Just over a decade later, the Court considered a similar fact pattern in *Lopez v. United States*.[481] This time, an agent from the Internal Revenue Service wore a recording device.[482] The Court rejected the argument that the defendant had a "constitutional right to rely on possible flaws in the agent's memory, or to challenge the agent's credibility without being beset by corroborating evidence that is not susceptible of impeachment."[483] To the contrary, "the risk that petitioner took in offering a bribe . . . fairly included the risk that the offer would be accurately reproduced in court, whether by faultless memory or mechanical recording."[484] The device had not intercepted new information.[485] It had just allowed for the information that was conveyed to the informer to be relayed more accurately in court.

The pattern continued. In *Hoffa v. United States*, the Supreme Court determined that a government informant relaying conversa-

477. *Id.* at 744.
478. 343 U.S. 967, 969 (1952).
479. *Id.* at 970.
480. *Id.* at 971.
481. 373 U.S. 427 (1963).
482. *Id.* at 430.
483. *Id.* at 439.
484. *Id.*
485. *Id.*

tions to federal law enforcement agents did not violate the Fourth Amendment, on the grounds that Jimmy Hoffa invited the informant into the room.[486] In *Lewis v. United States*, the Court again ruled the evidence admissible on the grounds that the defendant had invited the undercover agent into his home on numerous occasions.[487] These cases emphasized the voluntariness of the person confiding information in another person.

The informant cases also came down on the side of encouraging, rather than discouraging, the collection of *more accurate* information. That it was done with the aid of technology, and not via ordinary recall using human capacities, mattered little. In the Court's view, it was not different information that was being obtained, but simply information that more closely reflected what actually occurred. If it could be heard in the first place, then whether or not the brain had the ability to recall such detailed information was of little or no consequence.

Katz did little to alter the Court's view of the recording of information. Justice White cited the informant cases in his concurrence, stating (in dicta) that they had been "undisturbed" by the Court's ruling.[488]

Subsequent cases substantiated Justice White's claim. In 1971, in *United States v. White*, law enforcement officers recorded conversations between an informer and a suspect.[489] When the informer could not be located for the trial, the prosecution substituted the electronic recording.[490] The Court found no Fourth Amendment issue: "[A] police agent who conceals his police connections may write down for official use his conversations with a defendant and testify concerning them, without a warrant authorizing his encounters with the defendant and without otherwise violating the latter's Fourth Amendment rights."[491]

For the Supreme Court, there was no difference among an informer (a) writing down his recollections of the conversation, (b) recording the conversation with equipment secreted on his person, or (c) carrying equipment that transmitted the conversation to law enforcement officers or to recording devices.[492] The Court ex-

486. 385 U.S. 293, 302 (1966).

487. Lewis v. United States, 385 U.S. 206, 212 (1966).

488. Katz v. United States, 389 U.S. 347, 363 n.** (1967) (White, J., concurring).

489. 401 U.S. 745, 746–47 (1971) (plurality opinion).

490. *Id.*

491. *Id.* at 751 (citing Hoffa v. United States, 385 U.S. 293, 300–03 (1966)).

492. *Id.*

plained, "If the conduct and revelations of an agent operating without electronic equipment do not invade the defendant's constitutionally justifiable expectations of privacy, neither does a simultaneous recording of the same conversations made by the agent or by others from transmissions."[493] In undertaking criminal enterprises, one of the risks is that those with whom one deals are untrustworthy. While the informer's unavailability at trial might raise evidentiary problems or introduce potential questions of prosecutorial misconduct, it was immaterial as to whether the recording itself invaded the target's Fourth Amendment rights.[494] There was no appreciable difference between someone witnessing something happen and later recording it, and documenting what was said real-time, by, or with the consent of, individuals privy to the conversation.

Translated into private/public space doctrine, the potential for the government to record activity would fall outside the confines of the Fourth Amendment. What a police officer—or, indeed, any citizen—could witness in public would incur no further intrusion into an individual's privacy if the officer—or citizen—recorded it as it was happening.

In 1972, the Court confronted a similar private/public scenario and, in the context of the First Amendment, adopted a parallel approach. It was an era of civil unrest. The Department of the Army was called upon to assist local authorities in Detroit. Protesters brought a class action suit in District Court, seeking relief for their claim that the military's surveillance of lawful political activity undermined their First Amendment rights.[495] The data-gathering system used by the military placed the Army in a law enforcement role.

Just as the Court in the Fourth Amendment cases looked to the ability of ordinary citizens to access the same data as a metric for the scope of government power, so, too, did the Appellate Court and, later, the Supreme Court, look to ordinary police powers to assess what access to information should be provided to the military. The Court of Appeals explained, "To quell disturbances or to prevent further disturbances, the Army needs the same tools and, most importantly, the same information to which local police have

493. *Id.*

494. *White*, 401 U.S. at 754.

495. Laird v. Tatum, 408 U.S. 1 (1972).

access." Indeed, it may have even greater need than the local police, since they may be unfamiliar with the local population.[496]

The Army discharged its mission by collecting information about public meetings. It came from various sources:

> [T]he principal sources of information were the news media and publications in general circulation. Some of the information came from Army Intelligence agents who attended meetings that were open to the public and who wrote field reports describing the meetings, giving such data as the name of the sponsoring organization, the identity of speakers, the approximate number of persons in attendance, and an indication of whether any disorder occurred.[497]

Other information was derived from local police and other civilian law enforcement agencies.[498]

The Supreme Court considered—and rejected—the proposition that recording public meetings had any First Amendment chilling effect. To the contrary, the burden lay on those who attended the meetings to demonstrate the danger of direct injury.[499]

White dealt with taking notes from a recorded conversation.[500] The Supreme Court has not yet addressed video recordings or photographs. But two lower decisions have.

The first was the 1975 case of *Philadelphia Yearly Meeting of Religious Society of Friends v. Tate*.[501] The Philadelphia Police Department had amassed files on about 18,000 people and organizations, including information about their political views, personal associations, personal lives, and habits. In June 1970, officers publicly announced the names of some of the individuals who had been placed under surveillance. People involved brought suit, asserting that the practice of collecting information on citizens lacked any nexus to legitimate police purposes and deprived them of their right to anonymity with regard to their political activities and associations. The plaintiffs argued that the collection chilled their free exercise of speech and assembly and interfered with their abil-

496. *Id.* at 5 ("Since the Army is sent into territory almost invariably unfamiliar to most soldiers and their commanders, their need for information is likely to be greater than that of the hometown policeman.").

497. *Id.* at 6.

498. *Id.*

499. *Id.* at 14–15.

500. 401 U.S. 745, 746–47 (1971) (plurality opinion).

501. Phila. Yearly Meeting of Religious Soc'y of Friends v. Tate, 519 F.2d 1335, 1336–37 (1974).

ity to form lawful political associations that represented unpopular views.[502]

The District Court disagreed. Consistent with *Laird v. Tatum*, the fact that the police were engaged in an investigation did not chill the citizens' right to free speech.[503] The Court of Appeals reversed in part and affirmed in part, finding no additional Fourth Amendment interest.[504] "[M]ere police photographing and data gathering at public meetings" did not create any constitutional questions—nor did sharing it with other agencies with law enforcement interests.[505] Where the department went outside acceptable bounds was by going on national television and informing the public who they had under surveillance.[506]

This decision reflected the private/public distinction, and it accepted that the recording of the information itself did not change the quality of its collection as a matter of constitutional law. What is odd about the case is that the distinction it drew—namely with whom the information was *shared*—was determined *after* collection. It sidestepped whether the *recording* of the data in the first place qualified as a search within the meaning of the Fourth Amendment.

In the 1970s, the Fourth Circuit considered the potential First Amendment violation by law enforcement taking pictures at public meetings and demonstrations.[507] It was common practice at the time for police to photograph vigils, demonstrations, protests, and political meetings, regardless of whether they were peaceful or threatened violent behavior.[508] Judge Donald Russell, writing for the Court, determined that there had not been any constitutional intrusion.[509] He discounted any feeling of intimidation, citing to *Laird v. Tatum*, to claim that simply knowing one was under surveil-

502. *Id.* at 1337.

503. Phila. Yearly Meeting of Religious Soc'y of Friends v. Tate, 382 F.Supp. 547, 549 (1974); 408 U.S. 14 (Burger, J.), (noting that a broad-scale investigation was underway).

504. *Tate*, 519 F.2d at 1339.

505. *Id.* at 1337–38.

506. *Id.* at 1339 ("It cannot be doubted that disclosure on nationwide television that certain named persons or organizations are subjects of police intelligence files has a potential for a substantial adverse impact on such persons and organizations even though tangible evidence of the impact may be difficult, if not impossible, to obtain.").

507. Donohoe v. Duling, 465 F.2d 196, 197 (4th Cir. 1972).

508. *Id.* at 197–98.

509. *Id.* at 199.

lance was not sufficient to find a chilling effect.[510] The court was skeptical that those attending the rally really did feel intimidated by the presence of the cameras: "They did not object to being photographed; to the contrary, they solicited publicity both for their meetings and for themselves by inviting representatives of the news media, including photographers, to be present."[511] By holding a public meeting, in a public space, where ordinary citizens and news outlets would see and hear what was being said, the targets of the surveillance relinquished their right to prevent the government from recording what whey said and did.

In his dissent, Judge Winter distinguished the case from *Tatum*, noting that a number of individuals were photographed "without their permission and inferably against their will, while they were engaged in the peaceful exercise of their First Amendment right to assemble and [in some cases] to petition their government for a redress of their grievances."[512] In *Tatum* there was only knowledge of the surveillance program; in contrast, "here there was actual exposure to the challenged police methods."[513] That, in itself, provided "proof that actual harm and an actual violation of rights had occurred."[514]

The Chief of Police in Richmond, Virginia, and those who reported to him, decided which meetings to attend to identify leaders, to track people who may be travelling between meetings to stir up trouble, to deter violence and vandalism, and to protect peaceful demonstrators from counterdemonstrations.[515] Judge Winter was not persuaded that these objectives were furthered by the practice of photographing all attendees, or that the same objective could not be accomplished by means that did not interfere with otherwise protected First Amendment activities.[516] Law enforcement already knew who the leaders were, which made the efforts to intimidate the entire crowd concerning. He rejected the possibility that the police would use the photographs to identify unknown people.[517]

---

510. *Id.* at 201.

511. *Id.* at 200.

512. *Id.* at 204 (Winter, J., dissenting).

513. *Donohoe*, 465 F.2d at 205.

514. *Id.*

515. *Id.* at 206.

516. *Id.* at 207.

517. *Id.* at 206 ("I cannot suppose that every time a picture is taken of an unknown person it is sent to the FBI in order to determine whether that person is dangerous.").

Judge Winter's words appear almost quaint in an age of drones, big data, and biometric identification. In June 2015, the Associated Press reported that the Federal Bureau of Investigation (FBI) was using low-flying planes carrying video and cellphone devices.[518] Over a thirty-day period, the FBI flew the planes over more than thirty cities in eleven states across the country.[519] Using a quadcopter fitted with cameras, facial recognition technologies, and social media, it is conceivable that most people in a crowd could be instantaneously identified. Yet, under the current doctrine, even if a chilling effect might result, it might well be insufficient to prevent law enforcement from collecting the information. In the words of Justice Black in 1971:

> Where a statute [or police practice] does not directly abridge free speech, but – while regulating a subject within the State's power—tends to have the incidental effect of inhibiting First Amendment rights, it is well settled that the statute [or police practice] can be upheld if the effect on speech is minor in relation to the need for control of the conduct and the lack of alternative means for doing so.[520]

The recording of the information enhances the information beyond normal senses, or even the human brain. The data, moreover, can be combined with other input to construct detailed pictures of individuals' lives.

Far from appreciating the privacy interests entailed, the courts are refusing to acknowledge the considerable interests at stake.[521] In February 2016, the Sixth Circuit Court of Appeals considered a case in which law enforcement placed a suspect's home under surveillance for two and a half months.[522] In 2012, the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) had received a tip from the local sheriff in Tennessee that Rocky Houston, a convicted felon, had firearms at his residence. ATF, claiming that they were unable to observe the farm for any length of time because their cars "[stuck] out like a sore thumb," installed a camera at the top of a public utility pole overlooking his farm.[523] For ten weeks, the cam-

518. Associated Press, *FBI Using Low-Flying Spy Planes Over U.S.*, CBS NEWS (June 2, 2015), http://www.cbsnews.com/news/ap-fbi-using-low-flying-spy-planes-over-us/.

519. *Id.*

520. Younger v. Harris, 401 U.S. 37, 51 (1971).

521. *But see* United States v. Anderson-Bagshaw, 509 F. App'x 396 (6th Cir. 2012) (expressing "some misgivings" about the constitutionality of long-term warrantless surveillance of a backyard via a camera mounted on a pole).

522. United States v. Houston, 813 F.3d 282 (6th Cir. 2016).

523. *Id.* at 286.

era broadcast its recordings via an encrypted signal to an IP address accessed with a login and password.[524] At trial, ATF showed footage of Houston holding firearms seven times during the ten week period.[525]

The Court dismissed the possibility that any constitutional interest was at stake:

> There is no Fourth Amendment violation, because Houston had no reasonable expectation of privacy in video footage recorded by a camera that was located on top of a public utility pole that captured the same views enjoyed by passersby on public roads. The ATF agents only observed what Houston made public to any person traveling on the roads surrounding the farm.[526]

The length of the surveillance had no effect, "because the Fourth Amendment does not punish law enforcement for using technology to more efficiently conduct their investigations."[527] That technology made it easier and cheaper to track people for a longer time was of no consequence. "While the ATF agents could have stationed agents round-the-clock to observe Houston's farm in person, the fact that they instead used a camera to conduct the surveillance does not make the surveillance unconstitutional."[528]

If a member of the public could observe, with his/her naked eye, what was happening on the farm, the fact that the same person could observe it for weeks on end was unremarkable—as was the fact that the information happened to be recorded. So why could law enforcement not do the same? And if there was no privacy interest at the outset, then the fact that the observation went on for ten weeks at a time had little import. Zero plus zero equals zero.

This approach is disturbing in a digital age, in which the privacy interests implicated by new and emerging tracking technologies are considerable. It also sidesteps the important role that resource limitations have previously played in protecting citizens' privacy. Regardless of who is watching, ten weeks of surveillance implicates a range of privacy interests. As more information can be obtained from public space about the actions of individuals, incursions into the privacy sphere become deeper. The failure of Fourth Amendment doctrine lies in its inability to stem the steady constriction of the right to privacy based on the private/public distinction.

524. *Id.*
525. *Id.*
526. *Id.* at 286–88.
527. *Id.* at 288.
528. *Houston*, 813 F.3d at 288.

IV.
PERSONAL INFORMATION VERSUS THIRD-PARTY DATA

A second distinction in Fourth Amendment doctrine centers on the difference between private information and data entrusted to others. So-called "third-party doctrine" finds its origins in the informer cases, where the Court consistently held that information entrusted to others became divested of any privacy interest.

As aforementioned, in his concurrence in *Katz*, Justice White cited to *On Lee*, *Hoffa*, and *Lopez* in support of the proposition that what is exposed to other people implies an assumption of risk that the individual in whom one confides will make public what he has been told. As the Fourth Amendment does not protect against unreliable associates, "[i]t is but a logical and reasonable extension of this principle that a man take the risk that his hearer, free to memorize what he hears for later verbatim repetitions, is instead recording it or transmitting it to another."[529] White distinguished the informer cases from *Katz*, noting that in the case of the gambler, he had "'sought to exclude . . . the uninvited ear,' and spoke under circumstances in which a reasonable person would assume that uninvited ears were not listening."[530]

While White's concurrence sought to preserve the informer doctrine, it also laid the groundwork for third-party doctrine, which came to fruition in cases from the 1970s. *Miller v. United States*[531] and *Smith v. Maryland*,[532] and their progeny, stand for the proposition that while an individual may have an interest in information in her possession, as soon as it is conveyed to a third party, it no longer enjoys the same protections under the Fourth Amendment.

The concept of secrecy lies at the heart of the doctrine: what one keeps secret is private, while what one *voluntarily* exposes to others is no longer so. Relatedly, the most trenchant criticism of the private information/third-party data distinction revolves around the claim of *voluntariness*. In the contemporary world, it is impossible to live one's daily life without entrusting a significant amount of information to third parties.[533] To say that we therefore *voluntarily*

529. Katz v. United States, 389 U.S. 347, 363 n.** (1967) (White, J., concurring).

530. *Id.* (quoting *id.* at 351 (majority opinion)).

531. United States v. Miller, 425 U.S. 435, 443–44 (1976).

532. Smith v. Maryland, 442 U.S. 735, 744 (1979).

533. *See* Andrew William Bagley, *Don't Be Evil: The Fourth Amendment in the Age of Google, National Security, and Digital Papers and Effects*, 21 ALB. L. J. SCI. & TECH. 153, 154 (2011) (arguing that citizens are increasingly dependent on third party

assume the risk that such information will be made public denies the role that technology plays. This phenomenon can be thought of as "digital dependence."

A. Information Entrusted to Others

In 1976, the Court took up a critical question raised by *Katz*, which was whether the terrestrial distinction drawn at the border of the home would break down with regard to information held by a bank. In *Miller v. United States*, ATF suspected that Mitch Miller had failed to pay a liquor tax on whiskey and distilling equipment in his possession.[534] ATF agents served subpoenas on the Citizens and Southern National Bank of Warner Robins and the Bank of Byron to obtain Miller's financial records.[535] The banks subsequently provided all checks, deposit slips, financial statements, and monthly statements for grand jury deliberations.[536]

Justice Powell, delivering the opinion of the Court, cited back to *Hoffa* in support of the idea that an actual intrusion into a private sphere had to occur for a Fourth Amendment interest to be implicated.[537] He rejected any privacy interest in the records on the grounds that "checks are not confidential communications but negotiable instruments to be used in commercial transactions."[538] Powell underscored the voluntary nature of the relationship between Miller and the bank: "All of the documents obtained, including financial statements and deposit slips, contain only information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business."[539] Referencing the informer cases, Powell asserted, "The depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government."[540] He concluded, "Since no Fourth Amendment interests of the depositor are implicated here, this case is governed by the general rule that the issuance of a subpoena to a third party to obtain the records of that party does not violate the

service providers for their daily lives and suggesting that companies, in turn, are becoming increasingly intermingled with government agencies); Brenner, *supra* note 78, at 52–59 (underscoring the danger of failing to recognize any privacy interest in the rapidly expanding amount of information entrusted to third parties).

534. *Miller*, 425 U.S. at 436.
535. *Id.* at 437.
536. *Id.*
537. *Id.* at 440.
538. *Id.* at 442.
539. *Id.*
540. *Miller*, 425 U.S. at 443 (citing *White*, *Lopez*, and *Hoffa*).

rights of a defendant, even if a criminal prosecution is contemplated at the time the subpoena is issued."[541]

Justice Brennan strenuously objected to the Court's decision. He noted that the Supreme Court of California, which had a clause virtually *in haec verba* as the Fourth Amendment, had come to precisely the opposite conclusion. In *Burrows v. Superior Court*, a bank had voluntarily turned over an accused's financial records to the government.[542] The California Supreme Court had determined that individuals *do* have a reasonable expectation of privacy in their bank records, and Brennan agreed: "That the bank alters the form in which it records the information transmitted to it by the depositor to show the receipt and disbursement of money on a bank statement does not diminish the depositor's anticipation of privacy in matters which he confides to the bank."[543] The reasonable expectation was that, absent compulsion via legal process, whatever a customer reveals to a bank would only be used for internal banking purposes.[544] For the Supreme Court of California, whether or not a bank *voluntarily* turned its customer's records over to the police was irrelevant. Brennan agreed.

Justice Marshall also dissented in *Miller*, arguing, like Brennan, that the Bank Secrecy Act, which required banks to maintain customers' records, was unconstitutional on its face.[545] He also pointed out an apparent irony: while the majority in *California Bankers Association v. Shultz* had deemed the Fourth Amendment claims to be too premature to challenge the mandatory recordkeeping provisions in the statute, the Court now concluded that once the banks had been forced to keep customer records, any effort by the customer to assert a Fourth Amendment interest was too late.[546]

Three years later, the Court again considered third-party information in *Smith v. Maryland*.[547] In that case, Patricia McDonough had been robbed.[548] She provided a description of a 1975 Monte

541. *Id.* at 444.

542. *Id.* at 447–48 (Brennan, J., dissenting) (citing Burrows v. Superior Court, 529 P.2d 590, 593 (Cal. 1974)).

543. *Id.* at 448–49.

544. *Id.* at 449.

545. *Id.* at 455–56 (Marshall, J., dissenting).

546. *Miller*, 425 U.S. at 455 (Marshall, J., dissenting) (quoting California Bankers Ass'n. v. Shultz, 416 U.S. 21, 97 (1974) (Marshall, J., dissenting)).

547. Smith v. Maryland, 442 U.S. 735, 743–44 (1979); *see also* DONOHUE, FUTURE, *supra* note 6, at 119–21; Donohue, *Bulk Metadata*, *supra* note 6, at 868–69 (summarizing *Smith*).

548. *Smith*, 442 U.S. at 737.

Carlo parked at the scene of the crime to the police.[549] When she returned home, a man telephoned her repeatedly, identifying himself as the person who had robbed her, and threatening her.[550] At one point, he directed that she come out onto her porch, where she saw the Monte Carlo drive slowly past her home.[551] McDonough telephoned the police, who saw the vehicle and ran the plates, determining that it belonged to Michael Lee Smith.[552] They approached the telephone company and asked if it would be possible to put a pen register and trap and trace device on Smith's telephone line to see whether he was the person calling McDonough.[553] The telephone company agreed.[554] Within hours, Smith again telephoned McDonough. The police used the information to obtain a search warrant of Smith's home which, when executed, yielded a phone book, with a page turned down to McDonough's name.[555]

Citing *New York Telephone Company*,[556] the Court noted that the collection of the numbers dialed from the landline had not intercepted any content.[557] "Given a pen register's limited capabilities, therefore," Justice Blackmun wrote, the argument that the installation and use of a pen register constituted a search rested upon whether petitioner had a legitimate expectation of privacy in the numbers dialed from his phone.[558] The Court determined that he did not.[559]

For the Court, telephone subscribers knew, when dialing, that they were conveying the numbers to the company, since the information was required to connect the call.[560] They further realized that the company would make records of the numbers dialed.[561] This is what allowed customers to be billed for long-distance calls.[562] Similarly, even if most people were oblivious as to how telephone companies operated, they would nevertheless have some

549. *Id.*
550. *Id.*
551. *Id.*
552. *Id.*
553. *Id.*
554. *Smith*, 442 U.S. at 737.
555. *Id.*
556. *See* discussion, *infra*.
557. *Smith*, 442 U.S. at 741.
558. *Id.* at 742.
559. *Id.*
560. *Id.*
561. *Id.*
562. *Id.*

awareness that a pen register might be employed to identify individuals "making annoying or obscene calls."[563] The site of the call—in this case, inside the home—was immaterial:

> Although petitioner's conduct may have been calculated to keep the *contents* of his conversation private, his conduct was not and could not have been calculated to preserve the privacy of the number he dialed. Regardless of his location, petitioner had to convey that number to the telephone company in precisely the same way if he wished to complete his call.[564]

Even if the petitioner did have an expectation of privacy, the Court determined that he did not have one that society was willing to recognize as reasonable. Citing to *Miller*, as well as a string of informer cases (*Lopez*, *Hoffa*, and *White*), Justice Blackmun noted that the Court had consistently "held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[565]

Justice Stewart, joined by Justice Brennan, dissented, as did Justice Marshall, joined by Justice Brennan.[566] Stewart began by noting that in the years that had elapsed since *Katz*, telephones had become even more embedded in contemporary culture.[567] The fact that the telephone company used the numbers dialed for billing purposes said nothing about the underlying privacy interests. To place a call, individuals had to contract with the company. Yet the Court had recognized a privacy interest in the conversation conducted over the wires—even though the telephone company had the capacity to record it. Just because individuals *also* confided the number dialed to the telephone company, it did not follow that they necessarily had no interest in the information.[568] "I think," Stewart wrote, "that the numbers dialed from a private telephone—like the conversations that occur during a call—are within the constitutional protection recognized in *Katz*."[569] The numbers might be more prosaic than the actual conversation, but they were "not without 'content.'"[570] They could reveal the identities of those with

563. *Smith*, 442 U.S. at 742.

564. *Id.* at 743.

565. *Id.* at 743–44.

566. *Id.* at 746 (Stewart, J., dissenting); *Id.* at 748 (Marshall, J., dissenting).

567. *Id.*, 442 U.S. at 746 (Stewart, J., dissenting).

568. *Id.* at 746–47.

569. *Smith*, 442 U.S. at 747 (Stewart, J., dissenting).

570. *Id.* at 748.

whom an individual was in contact, divulging "the most intimate details of a person's life."[571]

Justice Marshall, in turn, attacked the Court's surmise that subscribers have no subjective expectation of privacy in the numbers dialed. Even assuming that they know that the company may monitor communications for internal reasons, it did not follow that they expected the company to turn the numbers dialed over to the public or to the government. "Privacy," he wrote, "is not a discrete commodity, possessed absolutely or not at all. Those who disclose certain facts to a bank or phone company for a limited business purpose need not assume that this information will be released to other persons for other purposes."[572]

Marshall raised further concerns that the Court's holding meant that those who contract with third parties assume the risk that the third party might disclose the information to the government. He laid forth two objections. First, "[i]mplicit in the concept of assumption of risk is some notion of choice."[573] In the informant cases, this was how the Court had considered the information later related during court proceedings. But in the case of a pen register, "unless a person is prepared to forego use of what for many has become a personal or professional necessity, he cannot help but accept the risk of surveillance."[574] It made no sense to talk about "assuming the risk," as if it were a choice, when, in order to live in the contemporary world, one in effect *had* no choice but to use a telephone.

Marshall's second objection was that risk analysis was an inappropriate tool. It allowed the government to set the contours of the Fourth Amendment. Under the Court's logic, "law enforcement officials, simply by announcing their intent to monitor the content of random samples of first-class mail or private phone conversations, could put the public on notice of the risks they would thereafter assume in such communications."[575] The question ought not to be what risks an individual presumably accepts by providing information to third parties, but what risks an individual "should be forced to assume in a free and open society."[576]

---

571. *Id.*

572. *Id.* at 749 (Marshall, J., dissenting) (citing his own dissent in California Bankers Assn. v. Shultz, 416 U.S. 21, 95–96 (1974)).

573. *Id.*

574. *Id.* at 750.

575. *Smith*, 442 U.S. at 750 (Marshall, J., dissenting).

576. *Id.*

Marshall's words proved prescient. He noted that the use of pen registers constituted "an extensive intrusion. To hold otherwise ignores the vital role telephonic communication plays in our personal and professional relationships."[577] Marshall's words harkened back to the majority in *Katz*, which had acknowledged the "vital role that the public telephone has come to play in private communication[s]."[578] Increasing dependence on the telephone meant that Fourth Amendment protections needed to come into play. For Marshall, the privacy rights of all citizens were at stake: "The prospect of unregulated governmental monitoring will undoubtedly prove disturbing even to those with nothing illicit to hide. Many individuals, including members of unpopular political organizations or journalists with confidential sources, may legitimately wish to avoid disclosure of their personal contacts."[579] The costs of allowing the government access to such data are borne in freedom of association and freedom of the press—both hallmarks "of a truly free society."[580] The government, moreover, was prone to abuse such powers: "Particularly given the Government's previous reliance on warrantless telephonic surveillance to trace reporters' sources and monitor protected political activity, I am unwilling to insulate use of pen registers from independent judicial review."[581]

B. Digital Dependence

In an era of increasing digital dependence, the arguments that Justices Stewart and Marshall put forth in *Smith v. Maryland* have become even more poignant.[582] To say that every time individuals

577. *Id.* at 751.

578. Katz v. United States, 389 U.S. 347, 352 (1967).

579. *Smith*, 442 U.S. at 751 (Marshall, J., dissenting).

580. *Id.*

581. *Id.* (footnote omitted). Following *Miller* and *Smith*, Congress passed two pieces of legislation that sought to create greater protections of privacy. *See generally* 12 U.S.C. §3401 (2013); Electronic Communications Privacy Act of 1986 (ECPA), Pub L. No. 99-508, 100 Stat. 1848 (codified as amended at 18 U.S.C. § 2510 (1986)). Further legislation has focused on cable subscriber and video store customer privacy. *See, e.g.*, Cable Communications Privacy Act of 1984, 47 U.S.C. § 551 (2006); Video Privacy Protection Act of 1988, 18 USC § 2710. But these measures only provide limited protections—and they have quickly become obsolete. ECPA, for instance, does not apply to the transmission of video. And stored content is only protected for six months.

582. Some scholars have argued, for similar reasons, for limits on subpoena powers. *See, e.g.*, Orin S. Kerr, *Digital Evidence and the New Criminal Procedure*, 105 COLUM. L. REV. 279, 309–10 (2005) (suggesting that "[t]he increase in the amount and importance of information stored with third parties in a network environment creates the need for new limits on the subpoena power," and arguing that "new

use their mobile phone they assume the risk that their data will be turned over to the government implies that people have no privacy interest in their communications, regardless of their substance and any effort to keep the information confidential.[583] But unlike the informer cases, where one has the capacity to mediate one's intimate relations, there is no meaningful choice in today's world as to whether or not a digital footprint is created as we go about our daily lives. Every time we make a call, drive our car, send an email, conduct an online search, or even walk down the street carrying a mobile device, we leave a trail.

For more than a decade, scholars have written about the changing world in which we live, raising the alarm that our increasing digital dependence is leading to a loss of privacy.[584] Nevertheless, the judiciary has failed to provide a backstop on the steadily diminishing zone of privacy that results from third party doctrine.[585] The Court's view, however, may be evolving.

In *United States v. Jones*, Justice Sotomayor suggested in her concurrence that in light of the deep privacy interests implicated by data entrusted to third parties, she might jettison third party doc-

---

rules should respond to the new privacy threats raised by third-party possession of private information made commonplace by computer networks and the Internet").

583. *See* Brenner, *supra* note 78, at 68 ("[T]he 'assumption of risk' calculus is an unreasonable methodology for a non-spatial world. It assumes . . . that I have a choice: to reveal information by leaving it unprotected or to shield it from 'public' view. In the real, physical world, these options make sense . . . . But how can I do this in a world of pervasive technology, a world in which I am necessarily surrounded by devices that collect data and share it with external entities?").

584. *See e.g.*, Patricia L. Belia & Susan Freiwald, *Fourth Amendment Protection for Stored E-Email,* 2008 U. CHI. LEGAL F. 121, 123–24 (2008); Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy,* 75 S. CAL. L. REV. 1083, 1084 (2002); *see also* Ilana R. Kattan, Note, *Cloudy Privacy Protections: Why the Stored Communications Act Fails to Protect the Privacy of Communications Stored in the Cloud*, 13 VAND. J. ENT. & TECH. L. 617, 619 (2011); Christopher R. Orr, Note, *Your Digital Leash: The Interaction Between Cell Phone-Based GPS Technology and Privacy Rights in* United States v. Skinner, 45 U. TOL. L. REV. 377, 377–78 (2014); *see generally* Bagley, *supra* note 534; Bellovin et al., *supra* note 447 at 559, n.8; Marc Jonathan Blitz, *The Fourth Amendment Future of Public Surveillance: Remote Recording and Other Searches in Public Space*, 63 AM. U. L. REV. 21, 26 (2013); Marc Jonathan Blitz, *Video Surveillance and the Constitution of Public Space: Fitting the Fourth Amendment to a World that Tracks Image and Identity*, 82 TEX. L. REV. 1349, 1353 (2004); Brenner, *supra* note 78; Jonathan Zittrain, *Searches and Seizures in a Networked World*, 119 HARV. L. REV. F. 83, 83 (2006).

585. Lower courts continue to hold the doctrinal line. *See, e.g.*, United States v. Graham, 846 F. Supp. 2d 384, 400 (D. Md. 2012).

trine altogether.[586] As aforementioned, in *Jones*, law enforcement had placed a GPS chip on a car without a warrant and tracked it for twenty-eight days.[587] Although the Court ruled on grounds of trespass, Sotomayor raised concern about the extent to which surveillance techniques that did not require physical intrusion impacted significant privacy interests. In light of the ubiquitous nature of digital technologies, she wrote, "it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties."[588] Citing to *Smith* and *Miller*, she recognized, "[t]his approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks."[589] Sotomayor explained:

> People disclose the phone numbers that they dial or text to their cellular providers; the URLs that they visit and the e-mail addresses with which they correspond to their Internet service providers; and the books, groceries, and medications they purchase to online retailers.[590]

Warrantless disclosures of, for instance, every web site visited over the past year surely held an implication for individual privacy. "[W]hatever the societal expectations," Sotomayor contemplated, "they can attain constitutionally protected status only if our Fourth Amendment jurisprudence ceases to treat secrecy as a prerequisite for privacy."[591] Not to put the point too bluntly, "I would not assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection."[592]

---

586. This view has been supported by a number of scholars. *See, e.g.*, Donohue, *supra* note 6, at 12; Susan W. Brenner & Leo L. Clarke, *Fourth Amendment Protection for Shared Privacy Rights in Stored Transactional Data,* 14 J. L. & POL'Y 211, 265 (2006). Others favor setting limits to keep it within the confines of the prevailing conditions in *Miller* and *Smith*. *See, e.g.*, Patricia L. Bellia, *Surveillance Law Through Cyberlaw's Lens*, 72 GEO. WASH. L. REV. 1375, 1407 (2004); Susan Freiwald, *First Principles of Communications Privacy*, 2007 STAN. TECH. L. REV. 3 ¶ 41 (2007); Deirdre K. Mulligan, *Reasonable Expectations in Electronic Communications: A Critical Perspective on the Electronic Communications Privacy Act*, 72 GEO. WASH. L. REV. 1557, 1578 (2004). Other scholars note that even if we jettison third party doctrine, significant difficulties remain. *See generally* Ohm, *supra* note 456, at 1330–32.

587. 132 S.Ct. at 948 (Scalia, J.).

588. *Id.* at 957 (Sotomayor, J., concurring).

589. *Id.*

590. *Id.*

591. *Id.*

592. *Id.*

The Supreme Court's continued emphasis on voluntary disclosure, and not on the government's *requirement* that the third party turn over the information in question, departs from the facts of *Smith* with lasting implications for individual rights. In that case, recall that the telephone company voluntarily relinquished the information to the government. Had the subscriber contracted with the company specifically to prevent the information from being forwarded to others, the individual would have had at least a contractually-protected right to prevent the information from being made available. The mere evidence rule, until 1967, would have prevented the forced disclosure of similar information by a warrant.

The Court has, at times, been at pains to distinguish the warrant process from the subpoena process. In the 1911 case of *Wilson v. United States*, the Court distinguished *Boyd v. United States*, in which the production "'of the private books and papers' of the owner of the goods sought to be forfeited" compelled him to be a witness against himself in violation of the Fifth Amendment and also amounted to an unreasonable search and seizure under the Fourth Amendment.[593] By contrast, the use of a "suitably specific and properly limited" writ, calling "for the production of documents which, as against their lawful owner to whom the writ is directed, the party procuring its issuance is entitled to have produced."[594]

It is important to recall here that the context for the subpoena power was the actual workings of either the grand jury or the court.[595] The difference between this context, and an investigation conducted by any law enforcement officer who obtains a warrant to obtain private information about individuals, is significant, indeed. By emphasizing the voluntariness of to whom the information is given, instead of the compulsion then exercised by the government on the entity providing the information, the Court misses an important way in which individual rights would otherwise have been guarded.

---

593. Wilson v. United States, 221 U.S. 361, 375 (1911) (quoting Boyd v. United States, 116 U.S. 616, 634–35 (1886)).

594. *Id.* at 376.

595. *See, e.g.*, Hale v. Henkel, 201 U.S. 43, 59–60 (1906) (allowing a grand jury to proceed to issue a subpoena absent a formal charge having been entered and relying on the oath given to the grand jury—that "you shall diligently inquire and true presentments make of all such matters, articles, and things as shall be given to you in charge, as of all other matters, and things as shall come to your own knowledge touching this present service," etc.—as demonstrating that "the grand jury was competent to act solely on its own volition").

At the same time, Sotomayor has it right, at least insofar as modern technology impacts the rights of individual actors.[596] Individuals do have a clear privacy interest in a range of data entrusted to corporate entities. But even where information may not appear to entail a privacy interest at the outset, when accumulated, much less when analyzed, possibly even in conjunction with other information, staggering insight into individuals' private lives may result.

V.
CONTENT VERSUS NON-CONTENT

As was discussed in Part II(B), prior to *Katz*, the Court determined that the contents of a letter deserved higher protection than the address on the outside of the envelope. This general framing (content versus non-content) gained ground after *Katz*. Technology, however, is now blurring the doctrinal distinction.

On the one hand, new forms of electronic communication (such as email, IMs, and text messages), which for all intents and purposes ought to be considered content, do not fall within the protections of the Fourth Amendment to the same degree that letters traditionally would—despite the fact that much of *the same information* is at stake.

On the other hand, data traditionally considered to be noncontent, such as pen register and trap and trace data, or envelope information, in light of digital dependence and the growth of social network analytics, generates a tremendous amount of information about individuals' relationships, beliefs, and predilections—precisely the interests that the distinction was meant to protect. The continued reliance on the content/noncontent distinction thus fails to capture the privacy interests at stake.

A. Electronic Communications

In *Katz*, the Court confronted whether an individual had a privacy interest in the contents of an individual's communications over

596. An argument could be mounted that "secrecy" is to an organization what "privacy" is to a natural person: namely, the right and the ability to keep individuals not part of the entity or privy to the relationship from knowing things. In some sense, "secrecy" and "privacy" thus represent the same interest expressed by different actors. Justice Sotomayor's formulation, however, considers third party doctrine to stand for the proposition that "secrecy" serves "as a prerequisite for privacy." The author understands her point as not being to confuse the two, but rather to suggest that the Constitutional right to individual privacy should not be premised upon the complete bar of anyone having access to the information in question.

a telephone line. In extending protections to the phone booth, the Court acknowledged the central role that telephones had come to play in the modern era.[597] Congress followed *Katz* with introduction of the 1968 Omnibus Crime Control and Safe Streets Act.[598] Title III laid out the rules that would henceforward govern the electronic intercepts. The law focused on the *content* of aural or wire communications.

While the Court has taken steps to protect the content of telephone communications, it has been slow to recognize a Fourth Amendment interest in *digital* communications.[599] The Supreme Court has not held, for instance, that individuals have a reasonable expectation of privacy in their e-mail. Instead, this realm is largely governed by statute.[600] Where the e-mail is located in the chain of communication alters how much statutory protection it receives. If an e-mail is sitting on a server and has not yet been read, for instance, it is subject to a different set of procedures than one that has been read. Similarly, if the e-mail is actually in transit, as opposed to just waiting to be read (or having been read), then it receives different protections. The complex statutes further take into account considerations such as the type of communications provider in possession of the information, and the length of time the communication has been stored.[601]

What makes the Court's failure to recognize a privacy interest in e-mail remarkable is not only the fact that e-mail conveys a significant amount of content, but that it lies at the very heart of early

---

597. Katz v. United States, 389 U.S. 347, 352 (1967); *see also* Smith v. Maryland, 442 U.S. 735, 751 (1973) (Marshall, J., dissenting).

598. *See* Berger v. New York, 388 U.S. 41, 63–64 (1967) (holding the New York wiretap law to be unconstitutional, precipitating federal legislation on the acceptable limits of wiretap authorities).

599. *But see* City of Ontario v. Quon, 560 U.S. 746, 762–63 (2010) (suggesting that "a search of [someone's] personal email account" would be as intrusive as "a wiretap on his home phone line").

600. Within the Electronic Communications Privacy Act (ECPA), the Wiretap Act, 18 U.S.C. §§ 2510-22 governs the interception of e-mail communications en route while the Stored Communications Act, 18 U.S.C. §§ 2701–12 (2012) regulates e-mails stored by certain entities.

601. For a good discussion of the different aspects of ECPA as applied to electronic communications, *see generally* CLANCY, *supra* note 79, at § 1.5. These nuances run counter to the Court's approach in *Ex parte Jackson*, discussed *infra*, in which the mere fact that a letter had left the home did little to alter the privacy interests entailed. An effort to amend the SCA failed in December 2012, when the Senate removed from proposed legislation a measure that would have stopped federal law enforcement from warrantless acquisition of e-mail. Adrian Fontecilla, *The Ascendance of Social Media as Evidence*, 28 CRIM. JUSTICE 1, 2 (2013).

21st century communications. By 2011, ninety percent of those using the Internet had sent or received e-mail, with half of the U.S. population using it daily.[602] E-mail has essentially replaced the paper correspondence at issue in *Ex parte Jackson*.

In the meantime, the lower courts remain divided. Some have come out in support of the proposition that e-mail falls within the remit of the Fourth Amendment. In 2008, the Ninth Circuit in *United States v. Forrester* recognized that "[t]he privacy interests in [letters sent through the post and email] are identical."[603] Two years later, the Sixth Circuit Court of Appeals catapulted the conversation forward in *United States v. Warshak*, finding that individuals do, indeed, have a reasonable expectation of privacy in their e-mail.[604]

Steven Warshak owned a company that sold an enormously popular product.[605] Its auto-ship program, however, failed to warn consumers that by requesting a free sample, they were being enrolled in a delivery schedule from which they would have to opt out to avoid being charged.[606] As complaints mounted, a grand jury returned a 112-count indictment against Warshak, ranging from mail, wire, and bank fraud, to money laundering.[607] In the course of its investigation, the government obtained 27,000 e-mails from Warshak's Internet Service Providers.[608] On appeal, Warshak argued that the warrantless seizure violated the Fourth Amendment.[609] The Court ultimately agreed, although it determined that, in this case, the government had relied in good faith on the Stored Communications Act, leaving the judgment undisturbed.[610]

In finding a Fourth Amendment interest, the Court observed, "[E]-mail was a critical form of communication among Berkeley

602. KRISTEN PURCELL, PEW RESEARCH CENTER, SEARCH AND EMAIL STILL TOP THE LIST OF MOST POPULAR ONLINE ACTIVITIES (Aug. 9, 2011), http://pewinternet.org/Reports/2011/Search-and-email.aspx; Matthew A. Piekarski, *E-mail Content's Brush with the Reasonable Expectation of Privacy: The Warshak Decision*, 47 U. LOUISVILLE L. REV. 771, 795 (2009).

603. United States v. Forrester, 512 F.3d 500, 511 (9th Cir. 2008).

604. United States v. Warshak, 631 F.3d 266, 274 (6th Cir. 2010).

605. *Id.* at 276. The product, Enzyte was "purported to increase the size of a man's erection." As the court noted, "[t]he product proved tremendously popular, and business rose sharply." By 2004, the company was making around $250 million per year.

606. *Id.* at 278.

607. *Id.* at 278, 281.

608. *Id.* at 282.

609. *Id.*

610. *Warshak*, 631 F.3d 266, at 282.

personnel."[611] Warshak, in particular, expected "that his emails would be shielded from outside scrutiny."[612] The Court continued, "given the often sensitive and sometimes damning substance of his e-mails, we think it highly unlikely that Warshak expected them to be made public, for people seldom unfurl their dirty laundry in plain view."[613]

The court underscored the relationship between written materials, telephone calls, and Internet communications. The growth of society's dependence on e-mail had shrunk the role of telephone calls and letters:

> People are now able to send sensitive and intimate information, instantaneously, to friends, family, and colleagues half a world away. Lovers exchange sweet nothings, and businessmen swap ambitious plans, all with the click of a mouse button. Commerce has also taken hold in email. Online purchases are often documented in email accounts, and email is frequently used to remind patients and clients of imminent appointments. . . . By obtaining access to someone's email, government agents gain the ability to peer deeply into his activities.[614]

The Fourth Amendment had to "keep pace with the inexorable march of technological progress, or its guarantees" would "wither and perish."[615]

"Over the last decade," the Sixth Circuit explained, "email has become 'so pervasive that some persons may consider [it] to be [an] essential means or necessary instrument[ ] for self-expression, even self-identification.'"[616] It required strong protections, without which the Fourth Amendment would not prove an effective guardian of private communication. It was not so much that e-mail had become an *additional* type of communication, as that it appeared to be *replacing* the traditional modes of communication, which increased the need for it to be protected.

The fact that the e-mail passed through an ISP was irrelevant. "If we accept that an e-mail is analogous to a letter or phone call, it is manifest that agents of the government cannot compel a commercial ISP to turn over the contents of an e-mail without trigger-

611. *Id.* at 283.

612. *Id.* at 284.

613. *Id.*

614. *Id.*

615. *Id.* at 285.

616. *Warshak*, 631 F.3d at 286 (quoting City of Ontario v. Quon, 560 U.S. 746, 760 (2010)).

ing the Fourth Amendment."[617] The ISP was an intermediary—the functional equivalent of a post office or telephone company. Just as law enforcement could not walk into a post office or a telephone company to demand the contents of letters or phone calls, neither could it demand that an ISP turn over e-mails absent a warrant.

Even as Sixth Circuit extended its protections to e-mail, it relied on the traditional content/non-content distinction. The court hastened to distinguish *Miller*, which involved "simple business records" used "in the ordinary course of business."[618] In contrast, the e-mails sent and received by Warshak were not directed to the ISP as an "intended recipient."[619]

The U.S. Court of Appeals for the Armed Forces (USCAAF) reached a similar conclusion with regard to the content of e-mails. In *United States v. Long*, it held that Lance Corporal Long had both an objective and a subjective expectation of privacy in e-mails retrieved from a government server.[620] The e-mails indicated that she had been afraid that "her drug use would be detected by urinalysis testing," and documented the steps she had taken to try to avoid discovery.[621]

USCAAF looked to *O'Connor v. Ortega*, in which the Supreme Court had recognized that government employees may have a reasonable expectation of privacy.[622] In *Long*, USCAAF acknowledged that the military workplace was not exactly the type of environment pictured in *O'Connor* (which had involved a physician at a state hospital).[623] Nevertheless, military personnel could, under some circumstances, have a reasonable expectation of privacy in their e-mail.[624] Long had used a password (one that the network adminis-

617. *Id.*

618. *Id.* at 288 (quoting United States v. Miller, 425 U.S. 435, 442 (1976)).

619. *Id.*

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

621. *Id.*

622. *Id.* at 61 (citing O'Connor v. Ortega, 480 U.S. 709, 716 (1987) (plurality opinion)). In *O'Connor*, the Court acknowledged that the reasonable expectation could be reduced with regard to the employee's office, desk, or filing cabinet in accordance with the "efficient and proper operation of the agency." It also recognized a lesser expectation where the search by the employer was related to workplace misconduct. *O'Connor* 480 U.S. at 720–22 (plurality opinion).

623. *Long*, 64 M.J. at 62; *O'Connor*, 480 U.S. at 712.

624. *Long*, 64 M.J. at 64. *See, e.g.*, United States v. Maxwell, 45 M.J. 406, 417 (C.A.A.F. 1996) (holding that Maxwell possessed a reasonable expectation of privacy in an America Online e-mail account). *But see* United States v. Monroe, 52 M.J. 326, 330 (C.A.A.F. 2000) (finding that because the e-mail system in question was owned by the government, Monroe had no contractual agreement guaranteeing privacy from those maintaining the e-mail system).

trator did not know) to access her account, establishing an expectation of privacy in her communications.[625] The fact that the e-mails were originally prepared in an office in Marine Corps' headquarters (HQMC), on a computer owned by the Marine Corps, and that the e-mails had been transmitted over the HQMC network, stored on the HQMC server, and retrieved by the HQMC network administrator, did not erode Long's Fourth Amendment rights.[626]

Although the Ninth and Sixth Circuits, and USCAAF, have extended an expectation of privacy to e-mail, others, looking at the "totality of the circumstances" have come to a different conclusion. In *United States v. Simons*, the Fourth Circuit relied upon the CIA's Foreign Bureau of Information Services's Internet policy, which restricted employees' use of the system to official government business and informed them of ongoing audits, to find that the Fourth Amendment did not apply.[627] The policy provided fair warning to employees and contractors that their use of the system might be monitored, even as it established the limits of how the system could be used. As a result, a government contractor who used the network to access and download photos from pornographic web sites could not claim the protection of the Fourth Amendment.[628]

The Fourth Circuit again determined in *United States v. Richardson* that AOL e-mail scans to detect child pornography, and the provision of that information to law enforcement, did not raise the specter of the Fourth Amendment.[629] AOL initiated its own process, outside of any government direction or control. As federal law enforcement neither required AOL to place e-mails under surveillance, nor directed how such searches should be conducted, no constitutional right came into being. The Fourth Amendment did not restrain private industry.

Similarly, in *United States v. Angevine*, the Tenth Circuit considered Oklahoma State University's log-on banner, which expressly disclaimed any right of privacy or confidentiality.[630] Together with "a computer policy that explains the appropriate computer use, warns employees about the consequences of misuse, and describes how officials monitor the University network," the banner provided

625. *Long*, 64 M.J. at 64–65.

626. *Id.* at 64.

627. United States v. Simons, 206 F.3d 392, 396 (2000).

628. *Id.*

629. U.S. v. Richardson, 607 F.3d 357, 364, 367 (4th Cir. 2010).

630. 281 F.3d at 1130, 1133 (2002).

sufficient notice to users that Fourth Amendment protections did not apply.[631]

As for text messages, as a doctrinal matter, it is far from clear whether they fall within Fourth Amendment protections. In 2010, the Supreme Court heard *City of Ontario v. Quon*, a case that centered on whether a government employer could read text messages sent and received on a pager owned by the government and issued to an employee.[632] In considering the reasonableness of the search Justice Kennedy, writing for the Court, recognized, "[C]ell phone and text message communications are so pervasive that some persons may consider them to be essential means or necessary instruments for self-expression, even self-identification."[633] He acknowledged, "[T]hat might strengthen the case for an expectation of privacy." But the very fact that the technology was so common and inexpensive meant that "employees who might need cell phones or similar devices for personal matters can purchase and pay for their own."[634] Employer policies, in turn, would shape the reasonableness of any expectations of privacy. The SWAT officer, whose messages had been read, had been told that he did not have any privacy rights in the pager system provided by the City of Ontario, California.[635] The Court did not address whether the content of text messages was protected.

At least one state supreme court has come to the conclusion that text messages do not trigger Fourth Amendment protections. In 2012, a lower Rhode Island state court held in *State v. Patino* that the defendant did have a reasonable expectation of privacy in the text messages sent and received.[636] In June 2014, the Rhode Island Supreme Court reversed the lower court's opinion.[637]

In *Patino*, police responded to a 911 call for a child who had stopped breathing.[638] Once the child was in the ambulance on the way to the hospital, the police looked through the mother's cell phone, which was laying on a kitchen countertop, and found texts

631. *Id.*

632. 560 U.S. 746 (2010).

633. *Id.* at 760.

634. *Id.*

635. *Id.* at 762 ("Even if he could assume some level of privacy would inhere in his messages, it would not have been reasonable for Quon to conclude that his messages were in all circumstances immune from scrutiny. Quon was told that his messages were subject to auditing.").

636. State v. Patino, No. P1-10-1155A, 2012 WL 3886269 (R.I. Super. Sept. 4, 2012), *aff'd in part, vacated in part*, 93 A.3d 40 (R.I. 2014).

637. State v. Patino, 93 A.3d 40 (R.I. 2014).

638. *Id.* at 43.

that incriminated the mother's boyfriend, Michael Patino.[639] The question before the court was whether individuals have a reasonable expectation of privacy in texts stored on *others'* cell phones.[640]

The court found that the reasonableness prong turned on whose phone was accessed.[641] Control mattered. "[W]hen the recipient receives the message," the court explained, "the sender relinquishes control over what becomes of that message on the recipient's phone."[642] Once the content of the message was revealed to another person, the sender lost any reasonable expectation of privacy. In this case, the police had accessed the owner's phone without her consent, although she had later signed a form allowing the police to search the device.[643] But for the Court, the sender had *already* relinquished any privacy interest and thus lacked standing to challenge the search and seizure of his messages.[644]

The Supreme Court has not affirmatively identified a Fourth Amendment interest in e-mail or text messages—to say nothing of instant messaging, or the myriad other ways that messages may be conveyed through apps, games, and other digital means.

In the 2014 case of *Riley v. California*, the Supreme Court was willing to acknowledge that a generalized privacy interest attached to a mobile phone in a search incident to arrest.[645] The case did not distinguish between the text messages on a phone and other functions, such as emails, address books, social media, or gaming applications.[646] Instead, it made a general argument that an immense amount of private information could be carried on a mobile device.[647] Several consequences for individual privacy followed:

> First, a cell phone collects in one place many distinct types of information that reveal much more in combination than any isolated record. Second, the phone's capacity allows even just one type of information to convey far more than previously possible. Third, data on the phone can date back for years. In

639. *Id.* at 45.

640. *Id.* at 55.

641. *Id.*

642. *Id.*

643. *Patino*, 93 A.3d at 56.

644. *Id.* at 57.

645. Riley v. California, 134 S. Ct. 2473, 2478 (2014).

646. *Id.*

647. *Id.* ("[M]odern cell phones have an immense storage capacity . . . . [They] can store millions of pages of text, thousands of pictures, or hundreds of videos.")

addition, an element of pervasiveness characterizes cell phones but not physical records.[648]

A generalized interest in cell phones, however, does not clearly establish the privacy interests that reside in the communication of digital content as transferred through e-mail, text messaging, and other means.

B. Pen Register/Trap and Trace Devices

Even as Supreme Court jurisprudence has, to date, failed to protect digital communications that look like traditional content, the growth of new technologies challenges the definition of certain types of non-content, because of the amount of content that they now convey. Perhaps the most ready example of this are pen register and trap and trace devices which the Court, in the aftermath of *Katz*, placed on the non-content side of the dichotomy. With the advance of technology and new algorithmic analyses, this type of information increasingly reveals intimate details about individuals' lives.

The first case directly on point arose in 1977, when the Court looked at whether a district court could direct a telephone company to assist in placing a pen register on a telephone line.[649] The Southern District of New York had issued an order authorizing the FBI to direct the telephone company to monitor two telephone lines, compensating the company for any assistance it was thereby forced to provide.[650] In *United States v. New York Telephone Co.*, the Court noted that the language of Title III did not cover the use of pen registers.[651] To the contrary, it was concerned only with orders "authorizing or approving the *interception* of a wire or oral communication."[652] Pen registers, the Court reasoned, "do not 'intercept,' because they do not acquire the 'contents' of communications."[653] The Court borrowed its understanding of "contents" from the statute itself, which understood it to include "any information concerning the identity of the parties to [the] communication or the existence, substance, purport, or meaning of [the] communication."[654] The Court cited the Senate Report, which explicitly dis-

648. *Id.* at 2478–79.
649. United States v. N.Y. Tel. Co., 434 U.S. 159, 161 (1977).
650. *Id.*
651. *Id.* at 166.
652. *Id.* (citing 18 U.S.C. § 2518(1)(1998) (emphasis added)).
653. *Id.* at 167.
654. *Id.* (citing 18 U.S.C. § 2518(1)(1998)).

cussed that the law was meant to exclude pen registers.[655] The action in question was consistent with the All Writs Act.[656]

Justice White, writing for the Court, outlined a number of considerations that made the use of the All Writs Act acceptable under the circumstances. First, the telephone company was not "a third party so far removed from the underlying controversy that its assistance could not be permissibly compelled."[657] Second, the Court had found probable cause that the facilities were being used to facilitate criminal activity on an ongoing basis.[658] Third, the assistance requested was "meager."[659] Fourth, the company was already "a highly regulated public utility with a duty to serve the public."[660] Fifth, "the use of pen registers" was "by no means offensive" to the telephone company.[661] Sixth, the company itself regularly used pen registers to check its billing operations, detect fraud, and prevent illegal activities.[662] Seventh, the order was not in any way burdensome, as it "provided that the Company be fully reimbursed at prevailing rates, and compliance with it required minimal effort on the part of the company and no disruption to its operations."[663] Eighth, without the company's assistance, the FBI could not have carried out its wishes.[664]

Justices Stevens, Brennan, Marshall, and Stewart all dissented in part from the Court's opinion.[665] Justice Stevens raised particular concern about jumping from the omission of pen registers and trap and trace devices in Title III to the conclusion that they were consti-

655. *N.Y. Tel. Co.*, 434 U.S. at 167–68 (quoting S. Rep. No. 90-1097, 90th Cong., 2d Sess. (1968) ("Paragraph 4 defines 'intercept' to include the aural acquisition of the contents of any wire or oral communication by any electronic, mechanical, or other device. Other forms of surveillance are not within the proposed legislation. . . . The proposed legislation is not designed to prevent the tracing of phone calls. The use of a 'pen register,' for example, would be permissible. *But see* United States v. Dote, 371 F.3d 176 (7th 1966). The proposed legislation is intended to protect the privacy of the communication itself, and not the means of communication.")).

656. *Id.* at 172 ("The Supreme Court and all courts established by Act of Congress may issue all writs necessary or appropriate in aid of their respective jurisdictions and agreeable to the usages and principles of law.") (quoting the All Writs Act, 28 U.S.C. § 1651(a) (2012)).

657. *Id.* at 174.

658. *Id.*

659. *Id.*

660. *Id.*

661. *N.Y. Tel. Co.*, 434 U.S. at 174.

662. *Id.* at 174–75.

663. *Id.* at 175.

664. *Id.* at 174–75.

665. *Id.* at 178.

tutionally authorized.[666] He pointed to *dicta* in *Katz*, which underscored that Rule 41 was not tied to tangible property.[667]

The content/non-content distinction highlighted in *New York Telephone Co.* persisted. The following year, in *Smith v. Maryland*, the Court returned to the function of pen registers as representing non-content, quoting *New York Telephone Co.* in support:

> [A] law enforcement official could not even determine from the use of a pen register whether a communication existed. These devices do not hear sound. They disclose only the telephone numbers that have been dialed—a means of establishing communication. Neither the purport of any communication between the caller and the recipient of the call, their identities, nor whether the call was even completed is disclosed by pen registers.[668]

Pen registers, and by inference trap and trace devices, represented non-content.

In an age of metadata and social network analytics, however, it simply is not true that data obtained via pen registers or trap and trace devices do not represent content.[669] A tremendous amount of information can be gleaned just from the numbers dialed and received by one's telephone. At the most obvious level, the numbers one dials reveal hobbies, interests, relationships, and beliefs. Contacting a drone manufacturer, or a 3D printer sales line shows an interest in drones and 3D printing. Calling a local political representative and members of the planning commission may show concern about development plans in the works. Repeated calls to a priest, rabbi, or imam—or to a church, synagogue, or mosque—may suggest religious conviction.

Communication patterns also reveal degrees of intimacy. Frequent contact with an individual denotes a closer relationship than those with whom one rarely interacts. Mapping the strength of these relationships, in turn, help to elucidate broader social net-

666. *Id.* at 179.

667. *N.Y. Tel. Co.*, 434 U.S. at 182–86.

668. 442 U.S. 735, 741 (1979) (quoting *N.Y. Tel. Co.*, 434 U.S. at 167).

669. Professor Orin Kerr has argued that while "the contents of online communications . . . should receive Fourth Amendment protection . . . non-content information should not be protected." Orin S. Kerr, *Applying the Fourth Amendment to the Internet: A General Approach*, 62 STAN. L. REV. 1005, 1007–08 (2010). The author disagrees with this argument on the grounds that the line between content and non-content, in a digital age, is often indiscernible. *See, e.g.*, Laura K. Donohue, *The Dawn of Social Intelligence (SOCINT)*, 63 DRAKE L. REV.1061, 1065 (2015).

works and an individual's relationship to others in the network.[670] From this, leaders can be identified. By mapping social networks, critical connections between different groups also can be identified.[671]

In June 2013, an associate professor of sociology at Duke University posted a provocative article, *Using Metadata to Find Paul Revere*, to illustrate the power of social network analytics.[672] Basing his analysis on the organizations to which the American Revolutionists belonged, Professor Kieran Healy identified shared membership of key organizations, in this manner uncovering the strength of relationships between key revolutionary groups. Breaking down his analysis further into the strength of individuals within and among organizations, Paul Revere emerges as the linchpin.[673] And Healy went further, calculating the eigenvector centrality number to evaluate the power of the various revolutionists, composing a short list of individuals who would be "persons of interest" to the Crown.[674] It neatly captured the most important members of the Revolution. Numerous studies similarly highlight that metadata reveals a tremendous amount of content, making Fourth Amendment doctrine appear almost quaint in a digital age.[675]

C. Envelope Information

Envelope information historically has not been considered within the gamut of the Fourth Amendment. Following *Katz*, the Court reiterated its protection of letters and packages.[676] Like communications placed inside envelopes, sealed packages provided to private carriers constitute "effects" within the meaning of the

670. *See generally* Greg Statell, *How the NSA Uses Social Network Analysis to Map Terrorist Networks*, DIGITAL TONTO (June 12, 2013), http://www.digitaltonto.com/2013/how-the-nsa-uses-social-network-analysis-to-map-terrorist-networks/.

671. Ronald L. Breiger, *The Duality of Persons and Groups*, 53 SOCIAL FORCES 181, 181–82 (1974).

672. Kieran Healy, *Using Metadata to Find Paul Revere*, KIERAN HEALY BLOG (June 9, 2013), https://kieranhealy.org/blog/archives/2013/06/09/using-metadata-to-find-paul-revere/.

673. *Id.*

674. *Id.*

675. *See, e.g.*, Declaration of Professor Edward W. Felten, ACLU v. Clapper, 959 F. Supp. 2d 724 (2013) (no. 13-cv-03994); Jonathan Mayer & Patrick Mutchler, *MetaPhone: The Sensitivity of Telephone Metadata*, WEB POLICY (Mar. 12, 2014), http://webpolicy.org/2014/03/12/metaphone-the-sensitivity-of-telephone-metadata/; *see also* Clifton B. Parker, *Stanford Students Show that Phone Record Surveillance Can Yield Vast Amounts of Information*, STANFORD REPORT (Mar. 12, 2014), http://news.stanford.edu/news/2014/march/nsa-phone-surveillance-031214.html.

676. Walter v. United States, 447 U.S. 649, 654 (1980).

Fourth Amendment.[677] What is written on the outside of the envelope or the package, though, does not enjoy a reasonable expectation of privacy. Underlying this approach is the basic concept that what one exposes to others who can simply observe the object, person, or behavior in question, does not fall within the Fourth Amendment. It is bolstered by the assumption that the address merely conveys to/from data—not content itself.

In an age of Internet communications, however, the argument that envelope information does not involve content breaks down. E-mail subject lines may carry significant details about the content of the messages themselves. Uniform Resource Locators (URLs) reveal the content of the pages for which one searches—and, therefore, what one reads. URLs reflect both the specific page being read and the website in general. Website IP addresses similarly reveal content. Yet the courts have yet to recognize the content conveyed through these digital resources, leaving electronic data unprotected from private or government intrusion.[678] In the interim, the government is seeking access to Internet browser history without a warrant.[679]

In *United States v. Hambrick*, the Fourth Circuit concluded that, under *Smith*, subscriber information conveyed to an ISP to set up an e-mail account was not protected.[680] The Ninth Circuit similarly held that the "to" or "from" addresses on e-mail, IP addresses of websites, or the total volume of file transfers linked to an Internet account, did not fall within the Fourth Amendment.[681] In *United States v. Forrester*, the Ninth Circuit focused on the distinction in *Smith* between content and non-content, concluding that the recording of IP addresses functioned as the constitutional equivalent of the pen registers in *Smith*.[682] The Court did acknowledge that the collection of not just website IP addresses but also URLs of

677. United States v. Jacobsen, 466 U.S. 109, 114 (1984).

678. Matthew J. Tokson, *The Content/Envelope Distinction in Internet Law*, 50 WM. & MARY L. REV. 2015, 2110–11 (2009).

679. *See, e.g.*, Ellen Nakashima, *FBI Wants Access to Internet Browser History Without a Warrant in Terrorism and Spy Cases*, WASH. POST (June 6, 2016), https://www.washingtonpost.com/world/national-security/fbi-wants-access-to-internet-browser-history-without-a-warrant-in-terrorism-and-spy-cases/2016/06/06/2d257328-2c0d-11e6-9de3-6e6e7a14000c_story.html.

680. United States v. Hambrick, No. 99-4793, 2000 WL 1062039, at *4 (4th Cir. Aug. 3, 2000).

681. United States v. Forrester, 495 F.3d 1041, 1048–49 (9th Cir. 2007).

682. *Id.*

pages visited "might be more constitutionally problematic," but it did not directly address the question.[683]

The Seventh Circuit came to a similar conclusion in *United States v. Caira*, finding that the government was not required to first get a search warrant before obtaining a suspect's IP address and login history from a third party provider.[684] Caira's efforts to draw a parallel to the GPS chip in *Jones* fell short: "The government received no information about how he got from home to work, how long he stayed at either place, or where he was when he was not at home or work. On days when he did not log in, the government had no idea where he was."[685] The cCourt acknowledged Justice Sotomayor's *Jones* concurrence, and her willingness to dispense with Third Party Doctrine altogether, but it also noted that the Supreme Court had yet to embrace her position.[686] Nevertheless, just as the GPS chip in *Jones* conveyed a significant amount of private information, so, too, do IP addresses and login histories.

One response to the privacy implications of collecting all of this data may be to simply assume that all digital information is content—driving the discussion to whether the information is public or private. Another response might be to say that no digital information is content. But this, too, ignores the deep privacy interests conveyed through bits and bytes. The current approach seeks to sort out the massive gray area between these two extremes. But simply re-entrenching the content/non-content distinction will not address the longer-term concern: how to protect the privacy interests at stake.

VI.
DOMESTIC VERSUS INTERNATIONAL

A final distinction that is breaking down in light of new and emerging technologies centers on the line between domestic and international. Until the mid-20th century, it was generally assumed that the Bill of Rights did not apply outside the United States, even when law enforcement sought to prosecute citizens for criminal activity overseas.[687] As the country expanded, only the territories that

683. *Id.* at 1049.

684. United States v. Caira, 833 F.3d 803, 809 (7th Cir. 2016).

685. *Id.* at 808.

686. *Id.* at 809

687. *See, e.g.*, *In re* Ross, 140 U.S. 453, 464 (1891) (holding that the Fourth Amendment was limited to domestic bounds); *see also* Jennifer Daskal, *The Un-Territoriality of Data,* 125 YALE L. J. 326, 336 (2015); Caitlin T. Street, Note, *Streaming the International Silver Platter Doctrine: Coordinating Transnational Law Enforcement in the*

were destined for statehood enjoyed the full protection of the Bill of Rights. Those that would remain unincorporated territories only enjoyed the protection of fundamental rights—understood in 1901 as including those "inherent, although unexpressed, principles which are the basis of all free government."[688] In 1957, the Supreme Court shifted its position, suggesting that the Bill of Rights applied to U.S. citizens abroad.[689]

In the decades after *Katz*, scholars began debating the universal application of the Bill of Rights.[690] Some lower courts began moving in this direction as well.[691] But the optimism proved short-lived. In 1990, the Supreme Court issued an opinion limiting the application of the Fourth Amendment overseas.[692]

There were good reasons for drawing a line. The uncertainties of investigations overseas, the delicacy involved in diplomatic exchanges, the risk of tipping off criminals with political and other ties to foreign governments, questions of jurisdiction, and other concerns suggested that the same standards that marked the domestic realm should not apply outside U.S. bounds. Resultantly, the Court eschewed a warrant requirement, falling back upon the reasonableness standard for U.S. persons abroad. For non-U.S. persons abroad lacking a significant connection to the United States, the

---

Age of Global Terrorism and Technology, 49 COLUM. J. TRANSNAT'L L. 411, 429 (2010–2011). Thus, while the Fourth Amendment applied within the United States—regardless of whether the individual targeted was a U.S. citizen or not—it did not apply outside U.S. borders. *See, e.g.*, Sardino v. Fed. Reserve Bank of N.Y., 361 F.2d 106, 111 (2d Cir. 1966) ("The Government's [argument] that 'The Constitution of the United States confers no rights on non-resident aliens' is so patently erroneous in a case involving property in the United States that we are surprised it was made."), *cited in* Daskal, *supra* at 336 n.22.

688. Downes v. Bidwell, 182 U.S. 244, 291 (1901) (White, J., concurring).

689. Reid v. Covert, 354 U.S. 1, 5–6 (1957) ("The United States is entirely a creature of the Constitution. Its power and authority have no other source. It can only act in accordance with all the limitations imposed by the Constitution. When the Government reaches out to punish a citizen who is abroad, the shield which the Bill of Rights and other parts of the Constitution provided to protect his life and liberty should not be stripped away just because he happens to be in another land.").

690. *See, e.g.*, Daskal, *supra* note 690, at 337–38; Louis Henkin, *The Constitution as Compact and as Conscience: Individual Rights Abroad and at Our Gates*, 27 WM. & MARY L. REV. 11, 34 (1985); Jules Lobel, *Here and There: The Constitution Abroad*, 83 AM. J. INT'L L. 871, 879 (1989); Paul B. Stephan III, *Constitutional Limits on the Struggle Against International Terrorism: Revisiting the Rights of Overseas Aliens*, 19 CONN. L. REV. 831 (1987).

691. *See, e.g.*, United States v. Conroy, 589 F.2d 1258, 1264 (5th Cir. 1979); United States v. Rose, 570 F.2d 1358, 1361–62 (9th Cir. 1978).

692. United States v. Verdugo-Urquidez, 494 U.S. 259, 261 (1990).

Fourth Amendment did not apply at all.[693] This, too, made sense, not just because of practical considerations, but also because a plausible reading of the Fourth Amendment understands "the people" to refer to citizens of the United States (see discussion, *infra*).

In the realm of national security, looser Fourth Amendment standards framed the collection of foreign intelligence within U.S. bounds.[694] Nevertheless, as in criminal law, the courts drew a line at the border, with no Fourth Amendment protections extended to U.S. persons located overseas.[695] In 2008, Congress took the first steps to acknowledge citizens' privacy interests outside the country. However, weaker standards apply than those that mark domestic collection.[696]

The problem is that persistent reliance on the borders of the country to protect citizens' constitutional rights fails to recognize that global communications systems run rampant over the domestic/international distinction. Where, previously, individuals would have to physically travel internationally, or deliberately put in telephone calls to other countries, thus entailing some level of knowledge that what one said or did was leaving the United States, today bits and bytes simply follow the most efficient route—without any deliberate action on the part of the individual generating the information. Much of the information generated internationally, moreover, is ultimately held in the United States or by U.S. entities—rather undermining the arguments that it is unpractical to obtain the same information, or that it would somehow alert foreign governments or criminals, by first requiring a warrant. Similarly, the implications for the jurisdictional argument fall away.

Nevertheless, because of the nature of global communications, and where the information is generated, the same types of communications that previously would have been protected are now more vulnerable to monitoring, interception, and collection by the government—simply because we live in a digital age.

---

693. *Id*. at 271.

694. *Compare* Title III of the Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. 90-351, 82 Stat. 197, codified at 18 U.S.C. §§ 2510-22 (standards for surveillance in the United States), *with* Foreign Intelligence Surveillance Act of 1978, Pub. L. 95-511, 92 Stat. 1783, codified at 50 U.S.C. § 1801 (standards for surveillance outside of the United States). *See also* discussion, *infra* pp. 86–88.

695. The 1978 Foreign Intelligence Surveillance Act purely addressed the collection of information on U.S. soil. Collection overseas fell within the broader framing of Executive Order 12,333.

696. Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008, Pub. L. 110-261, 122 Stat. 2436, July 10, 2008.

A. Law Enforcement

In 1990, the Supreme Court decided in *United States v. Verdugo-Urquidez* that non-U.S. citizens, who lack a substantial connection to the United States, do not enjoy the protections of the Fourth Amendment.[697] The DEA had conducted a warrantless search of Mexicali and San Felipe residences of a Mexican citizen.[698] Chief Justice Rehnquist, writing for the Court, suggested that the right of "the people" meant those who made up the political community of the United States—not non-citizens abroad, lacking a "substantial connection" to the country.[699]

Justice Kennedy, in his concurrence, pointed to the 1901 *Insular Cases*, a series of opinions addressing the status of Puerto Rico, the Philippines, and other overseas possessions, in which the Court had held that the Constitution does not apply in all its force to every territory under U.S. control.[700] While searches *within* the United States fell subject to the Fourth Amendment, practical barriers could prevent the same overseas.[701] Kennedy pointed to "[t]he absence of local judges or magistrates available to issue warrants, the differing and perhaps unascertainable conceptions of reasonableness and privacy that prevail abroad, and the need to cooperate with foreign officials" as reasons why "the warrant requirement should not apply in Mexico as it does in this country."[702]

Justice Brennan, joined by Justice Marshall, dissented.[703] How could the United States expand its extraterritorial criminal provisions without correspondingly allowing the Fourth Amendment to travel abroad? The fact that a foreign national was being investigated for a violation of U.S. law, for which he could conceivably "spend the rest of his life in a United States prison," was sufficient

697. *Verdugo-Urquidez*, 494 U.S. at 271, 274–75. *See also* Reid v. Covert, 354 U.S. 1, 5–6 (1957) (plurality opinion) (stating that the "shield" that the Bill of Rights provides "should not be stripped away just because [a U.S. citizen] happens to be in another land").

698. *Verdugo-Urquidez*, 494 U.S. at 262.

699. *Id.* at 271, 274–75.

700. *Id.* at 277 (Kennedy, J., concurring) (citing Downes v. Bidwell, 182 U.S. 244 (1901); Hawaii v. Mankichi, 190 U.S. 197 (1903); Dorr v. United States, 195 U.S. 138 (1904); Balzac v. Porto Rico, 258 U.S. 298 (1922)) (stating that the cases "stand for the proposition that we must interpret constitutional protections in light of the undoubted power of the United States to take actions to assert its legitimate power and authority abroad").

701. *Verdugo-Urquidez*, 494 U.S. at 278.

702. *Id.*

703. *Id.* at 279 (Brennan, J., dissenting).

to bring the Fourth Amendment to bear.[704] As soon as U.S. law applied, the foreign national became, "quite literally, one of the governed."[705] Fundamental fairness required that if individuals were obliged to comply with U.S. law, then the government, in turn, was "obliged to respect certain correlative rights, among them the Fourth Amendment."[706]

Under *Verdugo-Urquidez*, non-U.S. citizens based overseas, who lack a significant connection to the country, do not enjoy the protections of the Fourth Amendment.[707] Lower court decisions appear to come down on different sides of what, precisely, constitutes a "substantial connection."[708] For U.S. citizens outside the country, the Fourth Amendment *does* apply—albeit under different standards than those extended within the United States.[709]

The Supreme Court has not spelled out precisely what is required, although some lower courts have considered this question. In *United States v. Barona*, the Ninth Circuit determined that the Fourth Amendment only applies insofar as the search in question meets the reasonableness standard.[710] It does not demand that officials first obtain a warrant.[711] That case dealt with a DEA search conducted at the apex of the so-called "war on drugs," 1985–1987.[712] As the DEA had used electronic intercepts in accordance with Danish law, the court looked to whether the search was reasonable within the context of Denmark's legal framework, as

704. *Id*. at 283–84.

705. *Id.* at 284.

706. *Id.*

707. For discussion of this point and how the courts have subsequently answered the question of what constitutes a sufficient connection to the United States, see Laura K. Donohue, *Section 702 and the Collection of International Telephone and Internet Content*, 38(1) HARV. J. L. & PUB. POL'Y (2015), http://scholarship.law.georgetown.edu/facpub/1355/ [Hereinafter Donohue, *Section 702*].

708. *Compare, e.g.*, Martinez-Aguero v. Gonzalez, 459 F.3d 618, 625 (5th Cir. 2006) (finding substantial connections on the grounds that "regular and lawful entry . . . and [ ] acquiescence in the U.S. system of immigration constitute [ ] voluntary acceptance of societal obligations"), *with* United States v. Esparza-Mendoza, 265 F.Supp.2d 1254, 1271 (D. Utah 2003), *aff'd*, 386 F.3d 953 (10th Cir. 2004) (holding that "previously deported alien felons [who illegally re-enter the country] are not covered" under the sufficient connections on the grounds that he is "a trespasser in this country."); *see also* Donohue, *Section 702*, *supra* note 708; Orin S. Kerr, *The Fourth Amendment and the Global Internet*, 67 STAN. L. REV. 285, 291–93 (2015).

709. *See, e.g.*, United States v. Peterson, 812 F.2d 486, 490 (9th Cir. 1987).

710. 56 F.3d 1087 (9th Cir. 1995).

711. *Id.*

712. *Id*. at 1089–90. *See also* Donohue, Section 702, *supra* note 707, at 231-232.

well as whether U.S. officials had relied in good faith upon the foreign officials' representations that the wiretapping complied with Danish law.[713]

B. Foreign Intelligence Collection

Verdugo-Urquidez and *Barona* addressed ordinary law enforcement activity. For foreign intelligence collection, different standards apply, but they are still premised on a distinction between domestic and international searches. As with many of the authorities and cases addressed in this Article, the framing developed in a post-*Katz* world that no longer reflects the realities of a digital age.

In footnote 23 of *Katz*, the Court went out of its way to note that the decision did *not* reach national security cases.[714] Nevertheless, three justices took the opportunity to postulate what might be the appropriate standard for foreign intelligence collection. Justice White came down on the side of giving the Executive Branch more leeway.[715] Justice Douglas, in contrast, with whom Justice Brennan joined, distanced himself from White's view, which he considered "a wholly unwarranted green light for the Executive Branch to resort to electronic eavesdropping without a warrant in cases which the Executive Branch itself labels 'national security' matters."[716] Douglas recognized the potential conflict of interest in having the President or the Attorney General ultimately decide the limits of

713. *Id.* at 1094. *See also* Donohue, Section 702, *supra* note 707, at 232. The Second Circuit also found that the search of U.S. citizens overseas is only subject to the reasonableness requirement, and not the warrant clause. *In re* Terrorist Bombings of U.S. Embassies in East Africa, 552 F.3d 157, 171 (2d Cir. 2008). In *In re Terrorist Bombings*, American intelligence agencies had identified five telephone numbers used by individuals suspected of association with al Qaeda. *Id.* at 159 (*citing* United States v. Bin Laden, 126 F. Supp. 2d 264, 269 (S.D.N.Y. 2000). For a year, they monitored the lines, including ones used by an American citizen, El-Hage. In 1997, the Attorney General authorized intelligence officials to target El-Hage, placing his telephone line in his home in Nairobi, as well as his cell phone, under surveillance. U.S. officials later searched his home without a warrant. *Id.* at 160.

714. Katz v. United States, 389 U.S. 347, 358 n.23 (1967) ("Whether safeguards other than prior authorization by a magistrate would satisfy the Fourth Amendment in a situation involving the national security is a question not presented by this case.").

715. *Id.* at 364 (White, J., concurring) ("We should not require the warrant procedure and the magistrate's judgment if the President of the United States or his chief legal officer, the Attorney General, has considered the requirements of national security and authorized electronic surveillance as reasonable."); *see also* Donohue, *Section 702*, *supra* note 708.

716. *Katz*, 389 U.S. at 359 (Douglas, J., concurring); Donohue, *Section 702*, *supra* note 708.

their own powers.[717] The fact that the crimes in question were the most serious that could be alleged did little to alter his calculus.[718]

Congress responded to *Katz* by passing Title III of the Omnibus Crime Control and Safe Streets Act of 1968.[719] The legislation originally covered just wire and oral communications, but in 1986 Congress expanded it to include electronic communications. The Electronic Communications Privacy Act of 1986 included two additional titles focused on stored communications, as well as pen register and trap and trace devices.[720] Title III exempted matters involving national security:

> Nothing contained in this chapter . . . shall limit the constitutional power of the President to take such measures as he deems necessary to protect the Nation against actual or potential attack or other hostile acts of a foreign power, to obtain foreign intelligence information deemed essential to the security of the United States, or to protect national security information against foreign intelligence activities.[721]

Congress was careful to draft the law in a way that left the President's authority in the realm of foreign affairs intact.[722] Foreign in-

---

717. *Katz*, 389 U.S. at 359–60 (Douglas, J., concurring) ("Neither the President nor the Attorney General is a magistrate. In matters where they believe national security may be involved, they are not detached, disinterested, and neutral as a court or magistrate must be. Under the separation of powers created by the Constitution, the Executive Branch is not supposed to be neutral and disinterested. Rather it should vigorously investigate and prevent breaches of national security and prosecute those who violate the pertinent federal laws. The President and Attorney General are properly interested parties, cast in the role of adversary, in national security cases. They may even be the intended victims of subversive action.").

718. *Id.* at 360 ("Since spies and saboteurs are as entitled to the protection of the Fourth Amendment as suspected gamblers like petitioner, I cannot agree that, where spies and saboteurs are involved adequate protection of Fourth Amendment rights is assured when the President and Attorney General assume both the position of 'adversary and prosecutor' and disinterested, neutral magistrate.").

719. Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. 90-351, 82 Stat. 197, codified at 42 U.S.C. § 3711.

720. Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848, 1860, 1868 (codified as amended 8 U.S.C. §§ 2701, 3121 (1986)).

721. Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, 82 Stat. 197, 214 (1968).

722. 114 Cong. Rec. 14751 (1968) (Senators Holland, McClellan, and Hart stating that the legislation neither expanded nor contracted the President's foreign affairs powers); S. Rep. No. 90-1097, at 65 (1968) (stating that the power of the president "is not to be deemed disturbed" by the legislation). *See also* Donohue, *Section 702*, *supra* note 708, at 208.

telligence collection would be subject to different standards. Precisely what had yet to be decided.

In 1972, the Court weighed in on the question. In *United States v. United States District Court for the Eastern District of Michigan*, the Court suggested that in cases of domestic security, while some sort of judicial process was required for domestic interception, the standard could differ from criminal law.[723] The government had conducted a warrantless wiretap on three people suspected of bombing a Central Intelligence Agency office.[724] The Court agreed 8-0 that under the circumstances, the Government first had to obtain a warrant.[725] The Court cited the "inherent vagueness of the domestic security concept" as well as the risk of government abuse of power as reasons why the Fourth Amendment prevailed.[726] While the Government had to use what technological means it had at its disposal to protect citizens, giving the Executive Branch carte blanche undermined citizens' rights.[727]

Just as Justice Douglas in *Katz* had argued about the conflict of interest that marked giving the Executive the latitude to set the contours of its own power, Powell argued in *Keith* that, "Fourth Amendment freedoms cannot properly be guaranteed if domestic security surveillances may be conducted solely within the discretion of the Executive Branch."[728] Some sort of judicial process was necessary.[729] The precise contours lay in the domain of the legislature. "Different standards," Powell wrote, "may be compatible with the Fourth Amendment if they are reasonable both in relation to the legitimate need of Government for intelligence information and the protected rights of our citizens."[730] In criminal law, probable cause was the standard against which reasonableness was weighed; for foreign intelligence, the probable cause requirements may reflect "other circumstances more appropriate to domestic security

723. 407 U.S. 297, 322 (1972) [hereinafter *Keith*]; *see also* Donohue, *Section 702*, *supra* note 708, at 209.

724. *Keith*, 407 U.S. at 299.

725. *Id.* at 298, 320.

726. *Id.* at 320; *see also* Donohue, *Section 702*, *supra* note 708.

727. *Keith*, 407 U.S. at 312; *see also* Donohue, *Section 702*, *supra* note 708.

728. *Keith*, 407 U.S. at 316–17; *see also* Donohue, *Section 702*, *supra* note 708, at 210.

729. *Keith*, 407 U.S. at 318; *see also* Donohue, *Section 702*, *supra* note 708, at 210.

730. *Keith*, 407 U.S. at 322–23; *see also* Donohue, *Section 702*, *supra* note 708, at 210.

cases."[731] It may require a special court, different timing and reporting requirements than those outlined in Title III, and other special considerations.[732]

The 1978 Foreign Intelligence Surveillance Act (FISA) served as Congress's riposte.[733] The legislation was to be the *only* way the Executive branch could engage in domestic electronic surveillance for foreign intelligence purposes.[734] It later expanded FISA to govern physical searches, pen register and trap and trace devices, and tangible goods.[735]

For each of these areas, FISA incorporated standards more lenient than those that mark criminal law. Instead of requiring probable cause that a crime had been, was being, or was about to be committed, for instance, before electronic surveillance could commence, it required only probable cause that an individual was a foreign power or an agent of a foreign power, and probable cause that they would use the facilities to be placed under surveillance, before a special order from the FISC would issue.[736] The courts repeatedly upheld FISA as compatible with the Fourth Amendment.[737]

---

731. *Keith*, 407 U.S. at 323; *see also* Donohue, *Section 702*, *supra* note 708, at 210.

732. *Keith*, 407 U.S. at 323.

733. Foreign Intelligence Surveillance Act of 1978, Pub. L. 95-511, 92 Stat. 1783, codified at §§ 1801–1812, 1821–1829, 1841–1846.

734. *See generally* Donohue, *Bulk Metadata*, *supra* note 6, at 776–93 (discussing the historical background, structure, and purpose of the FISA); DONOHUE, FUTURE, *supra* note 6, at 11.

735. Intelligence Authorization Act for Fiscal Year 1995, Pub L. No. 103-359, § 302(c), 108 Stat. 3423, 3445 (1994) (codified at 50 U.S.C. §§ 1821–1829) (physical searches); Intelligence Authorization Act for Fiscal Year 1999, Pub. L. No. 105-272, § 601, 112 Stat. 2396, 2404–2410 (1998) (codified at 50 U.S.C. §§ 1841–1846) (pen register and trap and trace devices); *Id.* § 602 (codified at 50 U.S.C §§ 1861–1862); *see also* Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act), Pub. L.107-56, U.S.C. § 1861, 115 Stat. at 287 (2001) (evolution of business records to tangible goods).

736. *Compare* Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, tit. III, § 802, 82 Stat. 212 (1968) (codified as amended at 18 U.S.C. §§ 2510–22 (2012)), *with* 50 U.S.C. §1805(b).

737. *See, e.g.*, United States v. Pelton, 835 F.2d 1067, 1074–76 (4th Cir. 1987), *cert denied*, 486 U.S. 1010 (1988); United States v. Ott, 827 F.2d 473, 475 (9th Cir. 1987); United States v. Badia, 827 F.2d 1458, 1464 (11th Cir. 1987); United States v. Truong Dinh Hung, 629 F.2d 908 (4th Cir. 1980); United States v. Abu-Jihaad, 531 F. Supp. 2d 299, 304 (D. Conn. 2008); United States v. Mubayyid, 521 F. Supp. 2d 125, 136 (D. Mass 2007); United States v. Megahey, 553 F.Supp. 1180, 1185–93 (E.D.N.Y.), *aff'd*, 729 F.2d 1444 (2d Cir. 1982), *and aff'd sub nom* United States v. Duggan, 743 F.2d 59 (2d Cir. 1984).

FISA stopped at the border of the United States. All foreign intelligence surveillance involving electronic intercepts (and later, physical searches, pen register and trap and trace, or tangible goods), could only be undertaken on domestic soil consistent with the requirements in the statute. Internationally, intelligence collection fell outside the statutory regime and stemmed from the President's Article II authorities. From 1981 until 2008, such acquisitions only had to comport with the guidelines laid out in Executive Order 12,333.[738] In 2008, Congress passed the Foreign Intelligence Surveillance Amendments Act (FAA), bringing electronic surveillance of U.S. persons overseas within the contours of FISA.[739]

Prior to enactment of the FAA, the Southern District of New York (S.D.N.Y.) considered in a counter-terrorism context whether a U.S. citizen placed under surveillance overseas was entitled to the full protections of the Fourth Amendment and determined that he was not.[740] In *United States v. Bin Laden*, the Court rejected the necessity of law enforcement first obtaining a warrant before placing either a landline or a mobile telephone under surveillance.[741] The Court concluded that because of the undue burden that it would place on the Executive Branch, foreign intelligence collection overseas fell into the "special needs" exception.[742] Because of the "intricacies" involved, courts were "ill-suited to the task of overseeing foreign intelligence collection."[743] It was difficult to predict the international consequences of wiretapping on foreign soil; other countries might not want to be seen as complicit with actions taken by the United States, and enemies might be alerted to investigations underway—not least by foreign officials sympathetic to their cause.[744] The potential for security breaches to occur was significant.[745]

738. *See* Exec. Order No. 12,333, 3 C.F.R. 200 (1981), *reprinted* in 50 U.S.C. § 401 app. at 44–51 (1982); *see also* Donohue, *Section 702*, *supra* note 708; DONOHUE, FUTURE, *supra* note 6, at 12.

739. FISA Amendments Act of 2008, 50 U.S.C. § 1181(b) (2008); *see also* Protect America Act of 2007, Pub. L. No. 110-55, 121 Stat. 552 (temporarily bringing the collection of foreign intelligence targeting U.S. persons within the bounds of FISA); Donohue, *Section 702*, *supra* note 708.

740. *See Bin Laden*, 126 F. Supp. 2d at 264. *See* Donohue, *Section 702*, *supra* note 708.

741. *Bin Laden*, F. Supp. 2d at 275–76.

742. *Id*. at 274. *See also* Donohue, *Section 702*, *supra* note 707, at 233.

743. *Bin Laden*, F. Supp. 2d at 274.

744. *Id*. at 275. *See also* Donohue, *Section 702*, *supra* note 708.

745. *Bin Laden*, F. Supp. 2d at 275.

The S.D.N.Y. was careful to note the absence of any legislative framing.[746] The political branches, which were responsible for foreign affairs, had yet to create a warrant requirement for collection of intelligence abroad, making any judicial effort to do so somewhat suspect.[747] It was therefore up to the other two branches to work out the extent to which a warrant would be required and the specific procedures that would have to be followed for overseas collection. Deference, however, extended only insofar as collection centered on foreign intelligence.[748] As soon as the primary purpose of the search shifted to criminal law, ordinary Fourth Amendment standards for searches conducted overseas applied.[749]

In 2008, the Foreign Intelligence Surveillance Court of Review (FISCR) also considered whether a foreign intelligence exception to the warrant requirement existed for intelligence collected abroad.[750] FISCR pointed to its earlier opinion, which had assumed that regardless of whether a foreign intelligence exception to the warrant requirement existed, FISA met the Fourth Amendment standard of reasonableness.[751] It then turned to the question of whether, by a special needs analogy, there was a foreign intelligence exception to the warrant requirement.

FISCR emphasized the exceptional nature of national security, stating that the purpose behind foreign intelligence collection "goes well beyond any garden-variety law enforcement objective. It involves the acquisition from overseas foreign agents of foreign intelligence to help protect national security."[752] The court nevertheless rejected the proposition that the primary purpose of the investigation had to be related to foreign intelligence for the special needs exception to apply:

> [I]n our view the more appropriate consideration is the programmatic purpose of the surveillances and whether – as in

746. *Bin Laden*, F. Supp. 2d at 275–77. *See also* Donohue, *Section 702*, *supra* note 708, at 233-234.

747. *Bin Laden*, F. Supp. 2d at 275–77.

748. *Id*. at 277.

749. *Id. See also* Donohue, *Section 702*, *supra* note 708, at 234.

750. *In re* Directives Pursuant to Section 105B of the Foreign Intelligence Surveillance Act, 551 F.3d 1004 , 1012 (FISA Ct. Rev. Aug. 22, 2008); *see also* Donohue, *Section 702*, *supra* note 708, at 234-235.

751. *In re Directives*, 551 F.3d at 1011; *In re* Sealed Case, 310 F.3d 717, 744 (FISA Ct. Rev. 2002). *See also* Donohue, *Section 702*, *supra* note 708, at 235.

752. *In re Directives*, 551 F.3d at 1011. *See also* Donohue, *Section 702*, *supra* note 708, at 235.

> the special needs cases – that programmatic purpose involves some legitimate objective beyond ordinary crime control.[753]

Forcing the government to obtain a warrant would hurt its ability "to collect time-sensitive information and, thus, would impede the vital national security interests that are at stake."[754] For foreign intelligence collection, then, a different standard marks searches conducted overseas than those within domestic bounds.

The problem, as with criminal law, is that the distinction between domestic and international communications breaks down in light of new technologies.[755]

C. Technological Challenges to the Domestic/International Distinction

Global communications are, well, just that: global. They do not recognize terrestrial borders. Why conform Fourth Amendment requirements to geographic borders, when packets of information freely flow across them, and, for the most part, outside the control of users? The same information that would be protected under one framing falls subject to lesser protections under the other, despite the fact that the *same* communications are at stake—making Constitutional rights not so dependent on actual privacy needs, but on an accident of how the Internet works at any given time.

Consider, for instance, electronic mail communications. If I e-mail a colleague in the office next to mine, it may—or may not—be routed to a server in Singapore, where it awaits retrieval. *Pari passu*, foreign to foreign communications may be brought within the United States simply by being sent by the Internet across a U.S. frontier. In days of old, when telephone communications were carried on wires draped across land and water, one could intercept conversations entirely outside U.S. borders. But today, one scholar sitting in Dublin could e-mail a colleague in Bonn. And just as my e-

753. *In re Directives*, 551 F.3d at 1011. *See also* Donohue, *Section 702*, *supra* note 708, at 236.

754. *In re Directives*, 551 F.3d at 1011. *See also* Donohue, *Section 702*, *supra* note 708, at 237.

755. Although I focus on the physical characteristics (or lack thereof) of digital technologies, commentators also have focused on other ways in which technology has undermined Fourth Amendment doctrine as applied to searches outside the United States. *See, e.g.*, Street, *supra* note 688, at 429 n.72 (arguing that in the 21st century, "technology and the pervasive transnational terrorist threat have broadened the scope of the international silver platter doctrine, reduced the impact of its joint venture exception, and consequently rendered the Fourth Amendment, in practice, virtually inapplicable to most transnational terrorism investigations." The result is that more evidence obtained in unreasonable searches can be used in U.S. federal court.).

mail to a domestic colleague could go to Singapore, the e-mail from Dublin may be routed through Palo Alto, California. Does that mean that those communications now fall subject to higher levels of protection—either in the criminal law realm or in the foreign intelligence arena?

In 2008, Congress addressed the second part of the concern by enacting the FAA.[756] The government argued against extending higher Fourth Amendment protections to non-U.S. persons abroad simply because they chose to use a U.S. Internet service provider.[757] It was a sound argument. For one, it made little sense to have constitutional protections rest on the particular ISP involved, and not the status of the individual or the nature of the communication at stake. For another, if by simply using an American ISP, a foreign terrorist could gain greater protections, it would allow individuals to game U.S. law to evade detection.[758]

The problem that global communications present to Fourth Amendment law, however, works both ways. Even as communications overseas might be routed through the U.S., entirely domestic communications might now be routed overseas. If I email or text my colleague at Georgetown, the message may be routed through a server in Singapore before my colleague receives it. Through no action of my own, an entirely domestic message has traveled abroad. Yet it may be precisely the same message that, historically, if sent through regular mail, would have received full Fourth Amendment protections. So drawing a line at the border of the country, and extending fewer protections to the international communications, results in greater surveillance of U.S. citizens than has traditionally occurred.[759] The intense controversy surrounding Section

---

756. Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008, Pub. L. 110-261, 122 Stat. 2436, July 10, 2008; *see also* Donohue, *Section 702*, *supra* note 708; DONOHUE, FUTURE, *supra* note 6, at 33.

757. *Open/Closed Hearing: FISA Before the S. Select Comm. on Intelligence*, 110th Cong. (2007) (statement of John M. McConnell, Director of National Intelligence); *see also* 154 CONG. REC. H5756–57 (daily ed. June 20, 2008) (letter from Michael Mukasey, Attorney General, and J.M. McConnell, Director of National Intelligence, to Hon. Nancy Pelosi, Speaker, House of Representatives (June 19, 2008)); 154 CONG. REC. S6400–01 (July 8, 2008) (letter from Michael Mukasey, Attorney General, and J.M. McConnell, Director of National Intelligence, to Hon. Harry Reid, Majority Leader, Senate (July 7, 2008)); Donohue, *Section 702*, *supra* note 708.

758. *See also* Donohue, *Section 702*, *supra* note 708 (arguing that this was the strongest point put forward by the government in support of the FAA).

759. For discussion of this point, *see* Donohue, *Section 702*, *supra* note 708; *see also* Spencer Ackerman, *FBI Quietly Changes its Privacy Rules for Accessing NSA Data on Americans*, THE GUARDIAN (Mar. 8, 2016) (reporting PCLOB's confirmation that

702 of the FISA Amendments Act centered in no small measure on the government's inability to actually calculate the number of Americans whose privacy interests had been compromised even through upstream collection, directed at non-U.S. citizens abroad, and subsequent query of the database.[760]

It is more than just communications data at stake. Cloud computing, for instance, has altered where documents are not just stored but also analyzed.[761] There are increasingly difficult questions that center on whether and under what conditions the U.S. government can demand access to information held outside the United States. The Second Circuit confronted this question in regard to information linked to a Microsoft user's web-based e-mail account located in a data center in Dublin, Ireland.[762] A District Court determined that because the information could be obtained from Microsoft employees inside the United States, the warrant was not extraterritorial and thus valid.[763] The Second Circuit Court of Appeals, however, overruled this decision, stating that "to require a service provider to retrieve material from beyond the borders of the United States—would require us to disregard the presumption against extraterritoriality that the Supreme Court emphasized in

---

"the FBI is allowed direct access to the NSA's massive collections of international emails, texts and phone calls – which often include Americans on one end of the conversation"); *see generally* DONOHUE, FUTURE, *supra* note 6.

760. *See, e.g.*, PRIVATE & CIVIL LIBERTIES OVERSIGHT BD. REPORT ON THE SURVEILLANCE PROGRAM OPERATED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT 147 (2014) ("[L]awmakers and the public do not have even a rough estimate of how many communications of U.S. persons are acquired under Section 702."); James Ball & Spencer Ackerman, *NSA Loophole Allows Warrantless Search for U.S. Citizens' E-mails and Phone Calls*, THE GUARDIAN (Aug. 9, 2013), http://www.theguardian.com/world/2013/aug/09/nsa-loophole-warrantless-searches-email-calls; Elizabeth Goitein, *The NSA's Backdoor Search Loophole*, BRENNAN CENTER FOR JUSTICE (Nov. 14, 2013), https://www.brennancenter.org/analysis/nsas-backdoor-search-loophole; *Civil Society to FBI: Show Us How Section 702 Affects Americans*, PROJECT ON GOVERNMENT OVERSIGHT (Oct. 29, 2015), http://www.pogo.org/our-work/letters/2015/civil-society-to-fbi-show-us.html.

761. *See* Jessica Scarpati, *Big Data Analysis in the Cloud: Storage, Network and Server Challenges*, TECH TARGET, http://searchtelecom.techtarget.com/feature/Big-data-analysis-in-the-cloud-Storage-network-and-server-challenges (discussing the challenges of big data analytics in the cloud, including whether to move petabytes of data, as opposed to moving analytics to the data, to most effectively provide cloud-based services).

762. *In re* Warrant to Search a Certain E-mail Account Controlled and Maintained by Microsoft Corp., 15 F. Supp. 3d 466 (S.D.N.Y. 2014).

763. *Microsoft*, 15 F. Supp. 3d at 476; *see also* Jennifer Daskal, *The Un-Territoriality of Data,* 125 YALE L. J. 326 (2016).

Morrison v. Nat'l Austl. Bank Ltd., 561 U.S. 247 (2010)."[764] As Professor Jennifer Daskal, who has written thoughtfully about digital (un)territoriality, observed, "The dispute lays bare the extent to which modern technology challenges basic assumptions about what is 'here' and 'there.'"[765]

The problem with Fourth Amendment jurisprudence is that it assumes that one *can* draw a line at the border, and that the drawing of this line can be used in some meaningful way to determine the extent of constitutional protections. But, as Daskal notes, two aspects of the digital world make this impossible: first, data flows across borders at the speed of light and in unpredictable ways. Second, there is no necessary connection between where the data is located and where the individual that either "owns" the data, or to whom the data relates, is located, undermining the significance of where the data is at any moment in time.[766] Whether the individual to whom the data relates is a U.S. person, or a non-U.S. person lacking a significant connection to the United States (as framed in *Verdugo-Urquidez*), may be impossible to ascertain. No clearer is such a connection between bits and bytes flowing over the Internet and the citizenship or location of the foreign power at issue in FISA—even as amended.

Even if one had the IP address of a particular user, it is not at all clear from that information where a user is located—or even whether it is accurate. IP addresses are numerical sequences that can identify specific computers when they go online. They are used to route information to and from websites. But web anonymizers can hide IP addresses by creating a proxy, contacting the website on your behalf and forwarding the relevant information to you, so that no direct connection between your computer and the website is ever formed.[767]

With global communications, and the lack of digital technologies' territorial tie in mind, the concern is that the end result will be one in which the weaker standards previously adopted in regard to information obtained outside the United States become applied to an increasing amount of citizens' private data that happens to either flow across international borders, or to be held in foreign countries. This is the *de facto* standard already applied to foreign

764. Microsoft Corp. v. United States (*In re* Warrant to Search a Certain E-mail Account Controlled and Maintained by Microsoft Corp.), 829 F.3d 97, 201 (2d Cir. 2016).

765. *The Un-Territoriality of Data, supra* note 764.

766. *Id.*

767. *See e.g.*, WEB ANONYMIZER, http://www.webanonymizer.org.

intelligence collection and raises concerns about how the information is being used in a criminal law context—to say nothing about how the courts should consider criminal investigations when international data is involved.

VII.
CONFRONTING THE DIGITAL WORLD

The time is ripe to revisit the post-*Katz* distinctions—private vs. public; personal information vs. third party data; content vs. non-content; and domestic vs. international. They fail to capture the privacy interests affected by the digital sphere.

As this Article has argued, the ubiquitous nature of tracking technologies undermines the claim that what one does in public does not generate insight into private lives. Similarly, the rule that individuals lose their right to protect data when it is entrusted to others ignores the extent to which, as a society, we have become dependent on commercial entities to conduct our daily lives. If all information entrusted to third parties loses its constitutional protections, then the right to privacy itself will gradually cease to exist. Individuals *cannot* live in the modern world without creating a digital doppelganger that yields insight into our most intimate affairs. Denying the substantive interests involved in e-mail, texting, instant messages, and other forms of communication, moreover, subverts the purpose of distinguishing between content and non-content—even as technology has transmuted traditional areas of non-content to content. Global communications and cloud computing, in turn, collapse the line between what occurs inside the United States and that which transpires abroad.

The Court's continued reliance on these distinctions is leading to a narrowing of rights, with detrimental consequences for individual liberty.

There are a number of possible responses that the Court could make to the current situation in which we find ourselves. Prior to *Katz*, for instance, judicial doctrine reflected a textual approach, protecting "houses" and "papers" from the intrusive eyes of the government.

Accordingly, some scholars have suggested that digital information similarly should be considered "papers" and within the protection of the home, such that the *type* of information that would have been located behind closed doors falls within the ambit of the Fourth Amendment. The analogy runs: in a digital world, we no longer keep our papers in the den. Instead, we place them on the

cloud, encrypted. Whether the data is physical or digital should have little bearing on whether or not it is considered private. Either way, it is the same information in question.

A parallel approach centers on whether digital data ought to be considered within the domain of "effects."[768] As Professor Maureen Brady points out, compared to "houses" and "papers," "effects" has captured rather less of the Supreme Court's attention.[769] When it has, property considerations loom large.[770] In crafting a deeper understanding, Brady proposes that the Court look to the context, considering whether the subject of the inquiry is personal property, and whether the individual in question retains possession over it, rendering the property "presumptively entitled to Fourth Amendment protection."[771] This means looking beyond the actual location of the item—be it in a filing cabinet or on the cloud—and considering, instead, the nature of the item, its relationship to other items, and whether the owner has taken steps to shield the information from public scrutiny.[772]

A similar response centers on the Court's understanding of "persons." Much has been written about the "digital self"—doppelgangers that exist as a byproduct of living in the modern world.[773] As an extension of personhood, the digital self provides insight into one's intimate sphere. Under this approach, the collection of uniquely identifiable information, i.e., data that relates, and could be traced back, to unique individuals, may constitute a search per se, requiring a warrant for collection.

---

768. *See* Bagley, *supra* note 534, at 158 (looking at "the evolution of papers and effects increasingly stored by third party Internet giants").

769. Maureen E. Brady, *The Lost "Effects" of the Fourth Amendment: Giving Personal Property Due Protection,* 125 YALE L. J. 946, 980 (2016).

770. *Id*. at 981.

771. *Id.* at 951.

772. *Id.* at 952.

773. *See, e.g.*, SOLOVE, *supra* note 3; Jeremy N. Bailenson, *Doppelgangers: A New Form of Self*, 25 THE PSYCHOLOGIST 36, 36–39 (2012); Russell W. Belk, *Extended Self in a Digital World*, J. CONSUMER RESEARCH 477–500 (Oct. 2013); Hope Jensen Schau & Mary C. Gilly, *We Are What We Post? Self-presentation in Personal Web Space,* 30 J. CONSUMER RESEARCH 385 (2003); Nick Yee et al., *The Expression of Personality in Virtual Worlds*, 2 SOC. PSYCHOL. & PERSONALITY SCI. 5, 5–12 (2011); Nick Yee & Jeremy N. Bailenson, *The Difference Between Being and Seeing: The Relative Contribution of Self-Perception and Priming to Behavioral Changes via Digital Self-Representation*, 12 MEDIA PSYCHOLOGY 195 (2012); Nick Yee et al., *The Proteus Effect: Implications of Transformed Digital Self-Representation on Online and Offline Behavior*, 33 COMMUNICATION RESEARCH 271 (2009); Shanyang Zhao, *The Digital Self: Through the Looking Glass of Telecopresent Others*, 28 SYMBOLIC INTERACTION 387 (Aug. 2005).

The problem with these approaches is twofold: first, they do not directly confront the problems raised by the *Katz* reasonableness standard, discussed, at length, above. Second, more profoundly, they neither confront the theoretical framing of the Fourth Amendment, which presupposes a pre-political self, nor do they question the contemporary assumption that the purpose of the Fourth Amendment is to protect privacy.

In 2013, Professor Julie Cohen attacked the concept of a liberal self.[774] She argued that the real object of privacy law is a socially-constructed being, "emerging gradually from a preexisting cultural and relational substrate."[775] For Cohen, liberal political theory's commitment to definitions of absolute rights and core principles *is* the problem. It fails to acknowledge the types of privacy expectations that mark the real world.[776] "The self," Cohen writes, "has no autonomous, precultural core, nor could it, because we are born and remain situated within social and cultural contexts."[777] *Pari passu*, "privacy is not a fixed condition, nor could it be, because the individual's relationship to social and cultural contexts is dynamic."[778]

Cohen's insight illuminates Professor Anita Allen's observation that society's expectation of privacy appears to be changing.[779] "Neither individuals, institutions, nor government consistently demand or respect physical, informational, and proprietary privacy," Allen writes.[780] Thus, while polling data may show high levels of concern about privacy, "Certain legal and policy trends; certain modes of market, consumer, and political behavior; and certain dimensions of popular culture . . . suggest low levels of concern."[781] Allen cites to the "avalanche of technologies" that make information available to industry and the government.[782] She concludes, "Liberals may need to rethink the claims they have always made about the value of privacy."[783]

Cohen's approach offers a way out of Allen's conundrum. Instead of beginning from the point of political theory or philosophy,

774. Julie Cohen, *What Privacy Is For*, 126 HARV. L. REV. 1904 (2013).
775. *Id.* at 1905.
776. *Id.* at 1907.
777. *Id.* at 1908.
778. *Id.*
779. Anita L. Allen, *Coercing Privacy*, 40 WM. & MARY L. REV. 723, 727–28 (1999).
780. *Id.* at 728.
781. *Id.* at 729.
782. *Id.* at 730.
783. *Id.* at 728.

Cohen proposes that one must look to cognitive science, sociology, and social psychology to find the empirical foundations for understanding socially-constructed subjectivity.[784] In this framing, privacy plays a critical role, incubating subjectivity and independence, and wrenching individuals and communities from the clutches of governments and commercial actors that would relegate them to fixed, transparent, and predictable beings.[785] Perceived in this way, privacy "protects the situated practices of boundary management through which the capacity for self-determination develops."[786] The problem with a digitized, networked world, as it is currently constructed, is that it allows constant access to the boundary and therefore prevents the evolution of the socially-constructed self, outside of external influence.[787]

Cohen's conception of social construction as a theory of subjectivity differs in subtle but important way from other scholars who see privacy as socially constructed.[788] Professors Joshua Fairfield and Christoph Engel, for instance, try to turn the lens away from individuals in measuring harm. Instead, they draw attention to the negative externalities on non-consenting outsiders that are caused by the revelation of personal data.[789] Eschewing individualism, they argue, "it makes sense to examine privacy as a social construct, subject to the problems of social production."[790] They continue, "without measured intervention, individuals' fully informed privacy

784. Cohen, *supra* note 774, at 1908.

785. *Id.* at 1905.

786. *Id.*

787. *Id.* at 1916. ("In the contemporary information economy, private-sector firms like Google, Facebook, and data broker Acxiom use flows of information about consumer behavior to target advertisements, search results, and other content. . . . Information from and about consumers feeds into sophisticated systems of predictive analytics so that surveillant attention can be personalized more precisely and seamlessly. Government is an important secondary beneficiary of informational capitalism, routinely accessing and using flows of behavioral and communications data for its own purposes. . . . In the modulated society, surveillance is not heavy-handed; it is ordinary, and its ordinariness lends it extraordinary power.").

788. Professor Valerie Steeves highlights privacy as a social value, emphasizing its role in identity, dignity, autonomy, social freedom, and democracy. She considers the relationship between privacy and social equality, with particular emphasis on online social behavior. *See, e.g.*, Ian Kerr & Valerie Steeves, *Virtual Playgrounds and Buddybots: A Data-Minefield for Tinys and Tweeneys,* PANOPTICON, COMPUTERS, FREEDOM AND PRIVACY CONFERENCE (Apr. 12, 2005), http://idtrail.org/content/view/128/42/index.html.

789. Joshua A.T. Fairfield & Christoph Engel, *Privacy as a Public Good*, 65 DUKE L. J. 385 (2015).

790. *Id.* at 423.

decisions tend to reduce overall privacy, even if everyone cherishes privacy equally and intensely."[791] Applying a law and economics model, the scholars map the social and systemic harms that result from "the collection, aggregation, and exploitation of data."[792] Unlike Courts, which "tend to focus on specific harm to specific complaining individuals, not undivided losses to social welfare," economists conceive of harm differently.[793] A critical question is whether group harms "can be sufficiently theorized to be legally cognizable."[794]

If the approach to the liberal self that is built into Fourth Amendment doctrine is at least assailable, the object of the amendment is even more vulnerable to question, with profound implications for evolution of the doctrine.

Specifically, some scholars argue that the underlying value of the Fourth Amendment rests not on the right to privacy (either a liberal incarnation or one premised on social construction), but on *liberty from undue government power*.[795] Looked at in light of the history of the Fourth Amendment at the time of the Founding, this approach is extremely persuasive.[796] There is little question that Coke, Hale, and Hawkins, and other prominent English jurists and Parliamentarians, worried about limiting the power of the Crown.[797] It was to avoid the assumption and concentration of power that the common law came to restrict powers of search and seizure.[798] To place a limit on such powers, outside of hot pursuit of a known felon, the Crown could not enter into any home without a

---

791. *Id.*

792. *Id.*

793. *Id.* at 425.

794. *Id.* Other scholars similarly consider group privacy. *See, e.g.*, GROUP PRIVACY: NEW CHALLENGES OF DATA TECHNOLOGIES (Luciano Floridi, Linnet Taylor & Blair van der Sloot, eds. 2017). These theories, much like those posited by the Court in *Katz*, recognize that some aspect of privacy is socially constructed.

795. *See, e.g.*, DANIEL SOLOVE, NOTHING TO HIDE: THE FALSE TRADEOFF BETWEEN PRIVACY AND SECURITY, 1154 (Yale Univ. Press 2011) (focusing on the risks of government collection of information and centering the analysis on the type and extent of judicial oversight, limits on government actions, and guarding against abuse of power); Thomas Clancy, *What Does the Fourth Amendment Protect: Property, Privacy, or Security?*, 33 WAKE FOREST L. REV. 307, 351 (1998); Morgan Cloud, *The Fourth Amendment During the* Lochner *Era: Privacy, Property, and Liberty in Constitutional Theory*, 48 STAN. L. REV. 555, 618–19 (1996) (arguing that the Fourth Amendment "exists to enhance individual liberty by constraining government power").

796. *See* Donohue, *Original*, *supra* note 14.

797. *Id.*

798. *Id.*

warrant.[799] Neither a general warrant, nor one lacking the requisite particularity, would suffice.[800] The common law standard, of great importance to the founding generation, became codified in the U.S. Constitution.

In light of this history, it is perhaps unsurprising that in 2008, Professor Jed Rubenfeld observed an "oddity" in the Fourth Amendment: that privacy, "the 'touchstone' of modern Fourth Amendment law[,] fails to touch one of the paradigmatic abuses—arrests lacking probable cause made under a general warrant—that the Fourth Amendment was enacted to forbid."[801] The doctrine should simply give up "trying to protect privacy."[802] Instead, it should turn to what the real purpose was behind the amendment, which is a right of security.[803]

Rubenfeld's approach turns a cold shoulder to privacy as the determinant of Fourth Amendment protections. Other scholars take a similar line but are not quite as willing to throw the proverbial baby out with the bath water. Professor Paul Ohm, for instance, has argued that just as privacy replaced property, the Court should now consider power as the "constitutional lodestar" of the Fourth Amendment.[804] It is not that privacy is irrelevant to the Fourth Amendment enterprise—but rather that power ought to become a new interpretative lens for giving substance to privacy guarantees.[805]

Ohm is right to the extent that power ought to be considered the constitutional lodestar of the Fourth Amendment. But he is wrong in suggesting that it is a new interpretive lens. It is, instead, a return to the original values of the Fourth Amendment. And it offers a promising way forward for the Court to confront the significant threats posed by digitization, which carries with it the ability to record vast amounts of information, to combine information to

799. *Id.*

800. *Id.*

801. Jed Rubenfeld, *The End of Privacy*, 61 STAN. L. REV. 101, 104 (2008); *see also* Donohue, *Original*, *supra* note 14, at 1188–93 (discussing the original prohibition on general warrants).

802. Rubenfeld, *supra* note 802, at 104.

803. *Id.* at 104–05.

804. Ohm, *supra* note 456, at 1338.

805. Various efforts have been made to put alternative approaches into practice. *See generally, e.g.*, Kerr, *supra* note 35 (arguing that the rules ought to create a level playing field between criminals and law enforcement in light of technological advancement); Ohm, *supra* note 796 (building on Kerr by considering dual-assistance technologies that help both law breakers and law enforcement).

generate new knowledge, and to do so for many people over extensive periods of time, with minimal resource constraints.

In *Riley*, the Court alluded to these concerns.[806] It acknowledged four consequences that flowed from the government's collection of data, which helped to clarify why the search of a mobile phone was more invasive than finding a packet of cigarettes in someone's pocket. The former had "several interrelated privacy consequences."[807]

> First, a cell phone collects in one place many distinct types of information that reveal much more in combination than any isolated record. Second, the phone's capacity allows even just one type of information to convey far more than previously possible. Third, data on the phone can date back for years. In addition, an element of pervasiveness characterizes cell phones but not physical records. A decade ago officers might have occasionally stumbled across a highly personal item such as a diary, but today many in the more than 90% of American adults who own cell phones keep on their person a digital record of nearly every aspect of their lives.[808]

Similar issues haunted the shadow majority in *Jones*. Justice Alito recognized, "longer term GPS monitoring in investigation of most offenses impinges on expectation of privacy."[809]

Justice Sotomayor explained, "In cases involving even short-term monitoring, some unique attributes of GPS surveillance relevant to the *Katz* analysis will require particular attention."[810] That it was precise and reflected a "wealth of detail about" one's "familial, political, professional, religious, and sexual associations," was relevant.[811]

Sotomayor went on to note that the length of time the records could be kept, and mined, for more information, raised further concerns: "And because GPS monitoring is cheap in comparison to conventional surveillance techniques and, by design, proceeds sur-

806. *See also* Susan Friewald, *A First Principles Approach to Communications' Privacy*, STAN. TECH. L. REV. (2007) (arguing electronic surveillance that is intrusive continuous, indiscriminate, and hidden should be subject to Fourth Amendment restrictions). Friewald's principles align with the direction the Court took in *Riley* and *Jones*.

807. *Riley*, 134 S. Ct. at 2478.

808. *Id.*

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

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

811. *Id.*

reptitiously, it evades the ordinary checks that constrain abusive law enforcement practices."[812]

Justice Sotomayor tried to fold her broader concerns into the *Katz* framework: "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."[813] But in relying on *Katz*, Sotomayor's approach fell short of challenging the dichotomies and bringing attention to the underlying issue, which is the steady expansion of government power over the people. By acknowledging that the purpose of the Fourth Amendment was to protect against the accumulation of power, the Court will be better equipped to confront the dangers of the digital age.

812. *Id.* at 956.
813. *Id.*