0091-4169/13/10303-0745
THE JOURNAL OF CRIMINAL LAW & CRIMINOLOGY Vol. 103, No. 3

FIGHTING CYBERCRIME AFTER *UNITED STATES V. JONES*

DAVID GRAY,[*] DANIELLE KEATS CITRON[**] & LIZ CLARK RINEHART[***]

In a landmark nondecision last term, five Justices of the United States Supreme Court would have held that citizens possess a Fourth Amendment right to expect that certain quantities of information about them will remain private, even if they have no such expectations with respect to any of the information or data constituting that whole. This quantitative approach to evaluating and protecting Fourth Amendment rights is certainly novel and raises serious conceptual, doctrinal, and practical challenges. In other works, we have met these challenges by engaging in a careful analysis of this "mosaic theory" and by proposing that courts focus on the technologies that make collecting and aggregating large quantities of information possible. In those efforts, we focused on reasonable expectations held by "the people" that they will not be subjected to broad and indiscriminate surveillance. These expectations are anchored in

[*] Associate Professor, University of Maryland Francis King Carey School of Law.

[**] Lois K. Macht Research Professor of Law, University of Maryland Francis King Carey School of Law; Affiliate Scholar, Stanford Center on Internet and Society; Affiliate Fellow, Yale Information Society Project.

[***] University of Maryland Francis King Carey School of Law. The authors thank everyone who has generously commented on this work during presentations at Yale's Information Society Project, the Annual Meeting of the ABA/AALS Criminal Law Section, the University of North Carolina, Northwestern, Law and Society, and Yale's Conference on Locational Privacy and Biometrics, and during conversations at the Privacy Law Scholars Conference, the American Law Institute Meeting on Information Privacy Law, and Harvard's Symposium on Informational Privacy. Particular thanks go to Jack Balkin, Richard Boldt, Becky Bolin, Mary Bowman, Al Brophy, Andrew Chin, Bryan Choi, Thomas Clancy, Julie Cohen, Barry Friedman, LisaMarie Freitas, Susan Freiwald, Don Gifford, Mark Graber, James Grimmelmann, Deborah Hellman, Camilla Hrdy, Renée Hutchins, Orin Kerr, Joseph Kennedy, Catherine Kim, Anne Klinefelter, Michael Mannheimer, Dan Markel, Christina Mulligan, Richard Myers, Neil Richards, Catherine Sabbeth, Laurent Sacharoff, Paul Schwartz, Christopher Slobogin, Robert Smith, Dan Solove, Max Stearns, David Super, Peter Swire, Peter Quint, Arthur Weisburd, and Jonathan Witmer-Rich. As always, Frank Lancaster has been a rock.

Founding-era concerns about the capacity for unfettered search powers to promote an authoritarian surveillance state. Although we also readily acknowledged that there are legitimate and competing governmental and law enforcement interests at stake in the deployment and use of surveillance technologies that implicate reasonable interests in quantitative privacy, we did little more. In this Article, we begin to address that omission by focusing on the legitimate governmental and law enforcement interests at stake in preventing, detecting, and prosecuting cyberharassment and healthcare fraud.

TABLE OF CONTENTS

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[1]

I. INTRODUCTION

Until the middle of the October 2011 Term, the prevailing view on how to measure Fourth Amendment interests and where to draw the line between subconstitutional surveillance and a Fourth Amendment "search" focused on identifying "reasonable expectations of privacy."[2] If law enforcement officers did not enter private spaces, intrude on private interactions, or otherwise invade a defendant's subjectively manifested and objectively reasonable expectations of privacy, then they were left to pursue their investigations unfettered by Fourth Amendment constraints or concerns. Even if an investigative method or strategy did invade a person's reasonable expectations of privacy, the Fourth Amendment did not bar law enforcement officers from using it. Rather, the Fourth Amendment required that law enforcement's discretion be limited to ensure a reasonable balance between the government's interests and the privacy interests of those subject to search.

Until relatively recently, the contours of reasonable expectations of privacy, as well as the balance between law enforcement's interests and those of the individual, were fairly stable. In *United States v. Jones*[3] the Court indicated that the ground has begun to shift. As we have become more dependent on networked devices and as public spaces are increasingly tracked and traced, we expose more of ourselves to governmental actors and to third parties. As Justice Sotomayor noted in *Jones*, the government, by itself and through its contracted agents, now has access to powerful surveillance technologies and sophisticated software that is capable of aggregating and analyzing massive quantities of data.[4] For the most part, this literally occurs in bits and bytes that mean little when considered discretely. When aggregated together, however, these isolated events produce a revealing and disconcertingly vivid picture of our lives.[5]

---

[1] U.S. CONST. amend IV.

[2] Katz v. United States, 389 U.S. 347 (1967).

[3] 132 S. Ct. 945 (2012).

[4] *Id.* at 956 (Sotomayor, J., concurring).

[5] *See* David Gray & Danielle Citron, *A Shattered Looking Glass: The Pitfalls and Potential of the Mosaic Theory of Fourth Amendment Privacy*, 14 N.C. J.L. & TECH. (forthcoming 2013) (observing that "although a collection of dots is sometimes nothing more than a collection of dots, some collections of dots, when assessed holistically, are *A Sunday Afternoon on the Island of La Grande Jatte*").

Although *Jones* was resolved on narrow grounds, five Justices took the opportunity to suggest that these new surveillance capacities give law enforcement access to revealing informational mosaics that violate reasonable expectations of privacy and therefore implicate the Fourth Amendment. This "mosaic theory" of Fourth Amendment privacy is novel and will pose serious challenges for law enforcement officials, citizens, and courts if it is ultimately adopted.[6] Meeting these challenges will require, at a minimum, understanding both the privacy interests and the legitimate governmental interests at stake.

The concurring Justices in *Jones*, joined by academic commentators,[7] have described at length the privacy interests implicated by technologies capable of gathering large quantities of data. Almost absent from the discussion so far, however, has been any accounting of the legitimate governmental and law enforcement interests served by these technologies. That is unfortunate. After all, it is hard to strike a reasonable balance between the competing interests of law enforcement and citizen privacy, as the Fourth Amendment requires, if we lack a clear understanding of those competing interests. Our goal in this Article is to begin filling that void by discussing the role of data aggregation and surveillance technologies in the detection, investigation, and prosecution of cybercrimes.

The social problems constituting "cybercrime" are varied and costly. Take for example cyberharassment, which involves patterns of online behavior that are intended to inflict substantial emotional distress and would cause a reasonable person to suffer substantial emotional distress.[8] Multifaceted and malleable, "[c]yber harassment . . . tend[s] to involve explicit or implicit threats, privacy invasions, defamation, data thefts, impersonation, technological attacks, and[] the recruitment of third parties to physically harm victims."[9] Attackers hack into victims' computers to steal revealing pictures and then extort them, threatening to release the pictures unless they agree to the harassers' demands.[10] Vengeful ex-lovers

---

[6] For an in-depth discussion of the challenges, see *id.*

[7] *See, e.g.*, Christopher Slobogin, *Making the Most of* United States v. Jones *in a Surveillance Society: A Statutory Implementation of Mosaic Theory*, 8 DUKE J. CONST. L. & PUB. POL'Y 1 (2012); David Gray & Danielle Citron, *The Right to Quantitative Privacy*, 98 MINN. L. REV. (forthcoming 2013), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2228919.

[8] DANIELLE KEATS CITRON, HATE 3.0: THE RISE OF DISCRIMINATORY ONLINE HARASSMENT AND HOW TO STOP IT (forthcoming 2014). We include under this umbrella cyberstalking, which tends to have a more narrow definition—repeated online behavior, with intent to cause fear of bodily harm—as well as other forms of cyberharassment, including cyberextortion and other related offenses.

[9] *Id.*

[10] Another related cybercrime involves data theft. Harassers may hack into victims'

post victims' naked pictures on pornography sites alongside the suggestion that they are interested in anonymous sex.[11] Although some attackers confine their hostile activities to networked technologies, others use all available tools to harass victims, including real-space stalking.[12]

Cyberharassment has a profound impact on victims' lives. It causes debilitating psychological and emotional harm. It damages victims' careers and professional reputations. It interferes with their educations.[13] It silences them, discouraging them from on- and offline pursuits. In addition to psychological, emotional, and social damage, cyberharassment has led to sexual assaults, which are sometimes committed by unwitting third parties.[14]

Although fraud predates the computer by millennia, healthcare fraud provides an example of a traditional crime that has been upgraded and enhanced by new computer and Internet technologies. According to conservative estimates, approximately $60 billion in annual Medicare payments are fraudulent.[15] In sharp contrast, current efforts to prevent,

---

computers to steal their intimate images; crime rings use malware to harvest personal data and trade secrets from infected computers. The information is used to perpetrate identity theft, extortion, and industrial espionage. Steve Towns, *Strength in Numbers*, GOV'T TECH. MAG., Oct. 2012, at 18; Stephen Cobb, *Industrial Crimeware Sets a Blistering Pace*, SC MAG. (Aug. 22, 2012), http://www.scmagazine.com/industrial-crimeware-sets-a-blistering-pace/article/255601/.

[11] *See* United States v. Rose, 315 F.3d 956, 957 (8th Cir. 2003) ("Rose did in fact post pictures of [his victim's] children, along with their full names, address, and telephone number, on web sites soliciting sexual activity."); *see also* United States v. Sayer, Nos. 2:11-CR-113-DBH, 2:11-CR-47-DBH, 2012 WL 1714746, at *2 (D. Me. May 15, 2012) (explaining that in addition to uploading pornographic materials and the contact information of his victim, the stalker posted ads in her name "invit[ing] men to come to her home for sexual encounters") (citations omitted). Examples of "revenge porn" sites include Nik Richie's THE DIRTY.COM, which includes explicit posts like *The Dirtiest B*tch in Baltimore*, THE DIRTY (July 20, 2011), http://thedirty.com/2011/07/the-dirtiest-btch-in-baltimore/, and Hunter Moore's upcoming website HUNTERMOORE.TV, http://www.huntermoore.tv/, which is predicted to be a revival of his now-defunct ISANYONEUP.COM. Kashmir Hill, *Hunter Moore Will Post Your Nude Photos but Will Only Include Your Home Address if He Thinks You're a Horrible Person*, FORBES.COM (Dec. 5, 2012), http://www.forbes.com/sites/kashmirhill/2012/12/05/hunter-moore-is-going-to-start-posting-your-nude-photos-again-but-will-only-post-your-home-address-if-he-thinks-youre-a-horrible-person/.

[12] WORKING TO HALT ONLINE ABUSE, COMPARISON STATISTICS 2000–2012, at 3 (2012), *available at* www.haltabuse.org/resources/stats/Cumulative2000-2012.pdf.

[13] CITRON, *supra* note 8; Danielle Keats Citron, *Cyber Civil Rights*, 89 B.U. L. REV. 61, 71–73 (2009); Danielle Keats Citron, *Law's Expressive Value in Combating Cyber Gender Harassment*, 108 MICH. L. REV. 373, 382 (2009).

[14] *See* DeeDee Correll, *Craigslist Implicated in Rape Case: A Wyoming Man is Accused of Using the Website to Engineer an Ex-Girlfriend's Assault*, L.A. TIMES, Jan. 11, 2010, at A9.

[15] Kelli Kennedy, *U.S. Charges More than 100 in Wide Medicare Fraud Bust*, WASH.

detect, and prosecute healthcare fraud have produced only modest returns, recovering only $4.1 billion in 2011.[16] In addition to monetary costs, healthcare fraud also directly threatens the safety of patients, particularly when schemes result in unnecessary treatments, withholding necessary treatments, or disbursement of improper prescriptions.

There can be no doubt that the government has a compelling interest in detecting and prosecuting cybercrimes like cyberharassment and healthcare fraud. New and developing surveillance technologies, particularly those involving data aggregation and analysis, offer law enforcement officers helpful tools for combating these crimes. At the same time, these technologies implicate privacy interests that would be given Fourth Amendment status under a mosaic theory. In this Article, we explore these competing interests and outline ways that courts, legislatures, and executives might strike a reasonable balance between them. Part II provides a brief historical account of the relevant Fourth Amendment doctrine to put the mosaic theory in context and to explain the challenges it raises for identifying and balancing competing privacy and law enforcement interests. Part III focuses on the government's interest in preventing, detecting, and prosecuting healthcare fraud. Part IV elaborates on the government's significant interests in preventing, detecting, and prosecuting cyberharassment crimes. Part V concludes.

II. *UNITED STATES V. JONES* AND THE MOSAIC THEORY OF FOURTH AMENDMENT PRIVACY

To understand the new law enforcement dynamic set to take hold in cybercrime investigations and prosecutions, it is necessary to have a clear understanding of both the balancing test at the core of the Fourth Amendment and how the mosaic theory of Fourth Amendment privacy may put a thumb on that scale. That is the project for this Part.

As Akhil Amar has explored, agents conducting searches under state authority were subject to civil actions long before 1791.[17] The Fourth Amendment's prohibition on unreasonable searches and seizures draws on this common law history.[18] In fact, for the better part of a century after it was ratified, the Fourth Amendment appears to have been understood largely as a constitutional instantiation of property rights developed and

---

POST, Feb. 18, 2011, at A3.

[16] *About Fraud*, U.S. DEP'T OF HEALTH & HUMAN SERVS. & U.S. DEP'T OF JUSTICE, http://www.stopmedicarefraud.gov/aboutfraud/index.html (last visited May 21, 2013).

[17] Akhil Reed Amar, *Fourth Amendment First Principles*, 107 HARV. L. REV. 757, 786 (1994).

[18] Slobogin, *supra* note 7, at 12.

bundled through the common law of trespass.[19] So much so, in fact, that the prevalent remedy for Fourth Amendment violations until *Boyd v. United States*[20] was an action in tort.[21]

A trespass-based understanding of the Fourth Amendment may well have served the expectations of those who read the text in 1791. By the early years of the twentieth century, however, limiting the reach of the Fourth Amendment to physical incursions in protected places seemed inadequate. First, shifts in population from the farm to the city, coupled with the expansion of professionalized police forces, made routine, but nevertheless invasive, engagements with law enforcement far more common than our forebears living at the turn of the nineteenth century could have imagined.[22] Second, new technologies and their corresponding social expectations began to stretch common law concepts developed in the

---

[19] *See, e.g.*, Olmstead v. United States, 277 U.S. 438, 463 (1928) ("The well known historical purpose of the Fourth Amendment, directed against general warrants and writs of assistance, 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."). Orin Kerr has questioned this traditional understanding in a recent essay. *See* Orin S. Kerr, *The Curious History of Fourth Amendment Searches*, 2013 SUP. CT. REV. (forthcoming 2013), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2154611 [hereinafter Kerr, *Curious History*]. Without delving too far, we see less space between Professor Kerr's account and the orthodox view than he does. Although the Supreme Court often cited citizens' privacy interests in many of its pre-*Katz* cases, these interests were clearly tied to property. This is no surprise. After all, the common law has long understood property as a bundle of rights that can be variously acquired and alienated. These include the rights to exclude, to peaceful enjoyment, and to private use. Thus, as Professor Kerr himself has noted, the vast bulk of the Court's post-*Katz* cases have, in fact, focused on the privacy protections that citizens have in certain "places." *See* Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311, 316–17 (2012) [hereinafter Kerr, *Mosaic*].

[20] 116 U.S. 616 (1886).

[21] *See* Amar, *supra* note 17, at 774, 785–91; David Gray, *A Spectacular Non Sequitur: The Supreme Court's Contemporary Fourth Amendment Exclusionary Rule Jurisprudence*, 50 AM. CRIM. L. REV. (forthcoming 2013) (manuscript at 19), *available at* http://digitalcommons.law.umaryland.edu/cgi/viewcontent.cgi?article=2200&context=fac_pubs [hereinafter Gray, *Spectacular Non Sequitur*]; *see also* David Gray et al., *The Supreme Court's Contemporary Silver Platter Doctrine*, 91 TEX. L. REV. 7, 8–9 (2012) [hereinafter Gray, *Contemporary Silver Platter*]; William C. Heffernan, *The Fourth Amendment Exclusionary Rule as a Constitutional Remedy*, 88 GEO. L.J. 799, 808 (2000); Potter Stewart, *The Road to* Mapp v. Ohio *and Beyond: The Origins, Development and Future of the Exclusionary Rule in Search-and-Seizure Cases*, 83 COLUM. L. REV. 1365, 1372–77 (1983). Roger Roots recently has disputed this common wisdom. *See* Roger Roots, *The Originalist Case for the Fourth Amendment Exclusionary Rule*, 45 GONZ. L. REV. 1, 8–9 (2009–2010).

[22] *Olmstead*, 277 U.S. at 471–79 (Brandeis, J., dissenting); Wesley MacNeil Oliver, *The Neglected History of Criminal Procedure, 1850–1940*, 62 RUTGERS L. REV. 447, 460–61 (2010); *see also* DAVID R. JOHNSON, POLICING THE UNDERWORLD 4–9, 29–40 (1979) (describing how urbanization was a catalyst for the development of a modern police force and new investigative techniques).

context of cases involving physical intrusions into spaces traditionally protected by the common law of trespass.[23]

The facts of *Olmstead v. United States*[24] provide a useful example. A year after Bell and Watson's famous first telephonically transmitted words, there were 3,000 telephones in service in the United States.[25] The first coast-to-coast telephone line was completed in 1915.[26] Public telephones made their debut in the early 1880s, but took off after William Gray's invention of the coin-operated telephone in 1889.[27] In 1904, there were 3.3 million telephones in service in the United States.[28] Four years later, New York City alone had over 800,000 telephones.[29] By the time the "French phone" made its first appearance on the American market and AT&T opened the first transatlantic telephone service in 1927, the telephone had become a ubiquitous feature of American life.[30] As with all liberty-enhancing technologies, the telephone was also vulnerable to perversion in the hands of criminals. Where this occurred, law enforcement officers had a natural desire to listen in.

In *Olmstead*, law enforcement officers investigating a conspiracy to import and distribute intoxicating liquors "tapped" telephone lines using a crude version of today's surveillance tools: "[s]mall wires [that] were inserted along the ordinary telephone wires."[31] "The[se] insertions were made without trespass upon any property of the defendants."[32] Via these

---

[23] *Olmstead*, 277 U.S. at 471–79 (Brandeis, J., dissenting); Oliver, *supra* note 22, at 460–61.

[24] 277 U.S. at 438.

[25] *Telephone History: The Early Years 1876–1900*, TELEPHONY MUSEUM http://www.telephonymuseum.com/telephone history.htm (last visited May 21, 2013); *see also* TIM WU, THE MASTER SWITCH: THE RISE AND FALL OF INFORMATION EMPIRES 9–32 (2010).

[26] *Telephone History: The New Century 1901–1940*, TELEPHONY MUSEUM, http://www.telephonymuseum.com/History 1901-1940.htm (last visited May 21, 2013); *see also* WU, *supra* note 25.

[27] Sheldon Hochheiser, *Public Telephones*, IEEE USA TODAY'S ENGINEER (July 2009), http://www.todaysengineer.org/2009/jul/history.asp (last visited May 21, 2013); *see also* WU, *supra* note 25.

[28] *A Brief History: Origins*, AT&T, http://www.corp.att.com/history/history1.html (last visited May 21, 2013); *see also* WU, *supra* note 25.

[29] HERBERT N. CASSON, THE HISTORY OF THE TELEPHONE 172–73 (1910), *available at* http://etext.virginia.edu/etcbin/toccer-new2?id=CasTele.sgm&images=images/modeng&data=/texts/english/modeng/parsed&tag=public&part=5&division=div1; *see also* WU, *supra* note 25.

[30] *See, e.g.*, CLAUDE S. FISHER, AMERICA CALLING: SOCIAL HISTORY OF THE TELEPHONE TO 1940, at 52–53 (1992); *Getting the Radio News by Telephone*, 43 POPULAR MECHANIC 636, 636–38 (1925); *Hello London!*, 47 POPULAR MECHANIC 353, 353–54 (1927).

[31] Olmstead v. United States, 277 U.S. 438, 456–57 (1928).

[32] *Id.* at 457.

taps, the officers were surreptitiously able to listen to and record conversations among the conspirators, which allowed them to gather critical information about the conspiracy and to direct and target their interventions with maximum efficiency and safety. Based in part on information gathered through, or as a consequence of, these wiretaps, Olmstead and his confederates were prosecuted and convicted for a range of Prohibition-related offenses. Olmstead appealed, alleging that the installation and use of the wiretaps violated his Fourth Amendment rights. On certiorari to the United States Supreme Court, the absence of any physical trespass turned out to be determinative.

Writing for the majority in *Olmstead*, Chief Justice Taft found that all of the Court's prior Fourth Amendment decisions entailed either an "actual entrance into private quarters" or "the taking of something tangible."[33] Furthermore, he pointed out, the Amendment's enumeration of "persons, houses, papers, and effects," along with its requirement that warrants specify "the place to be searched, and the persons or things to be seized," limited the scope of its protections to "material things."[34] Because the surveillance technique employed by the officers in *Olmstead* did not entail a physical trespass, Chief Justice Taft saw no search or seizure.[35] Rather, in light of the fact that "[t]he evidence was secured by the use of the sense of hearing, and that only,"[36] the Court held that the "the wiretapping here disclosed did not amount to a search or seizure within the meaning of the Fourth Amendment."[37] Although Chief Justice Taft invited legislative intervention to set limits on law enforcement's use of wiretapping technologies,[38] he could see no constitutional authority for the Court to intervene in the absence of a physical trespass.[39]

In a prescient dissent from the majority opinion in *Olmstead*, Justice Brandeis argued that limiting Fourth Amendment protections to the compass of common law trespass failed to provide adequate protections for

---

[33] *Id.* at 457–64.

[34] *Id.* at 464.

[35] *Id.*

[36] *Id.*

[37] *Id.* at 466.

[38] The wiretapping at issue in *Olmstead* was conducted in violation of state law. *Id.* at 468–69. Over Justice Holmes's protest, *id.* at 470, however, the *Olmstead* majority maintained that state law could not dictate rules of evidence governing federal courts. *Id.* at 469.

[39] *Id.* at 465–66. Of course, that legislation was long in coming. It was not until 1968, after the Court abandoned the underlying rationale of *Olmstead* in *Katz v. United States*, 389 U.S. 347 (1967), that Congress finally stepped in, passing the Wiretap Act and then the Electronic Communications Privacy Act.

citizens at the dawn of a new technological age.[40] Although he acknowledged the Fourth Amendment's historical focus on physical trespass, Justice Brandeis argued that "a principle, to be vital, must be capable of wider application than the mischief which gave it birth."[41] Although "force and violence" had until then been a prerequisite for constitutional engagement, Justice Brandeis observed that "[s]ubtler and more far-reaching means of invading privacy have [since] become available to the Government."[42] Furthermore, he predicted that this trend would continue.[43] In the face of increasing hostility to privacy, Justice Brandeis refused to accept the majority's view that the Fourth Amendment had no say with regard to law enforcement's use of expanding surveillance capacities in ways that could threaten "the most comprehensive of rights, and the right most valued by civilized men": "the right to be let alone."[44]

In the years after *Olmstead*, many of Justice Brandeis's predictions about the expansion of government surveillance came to pass, and his views

---

[40] 277 U.S. at 473 (Brandeis, J., dissenting). Justice Brandeis's dissent came as no surprise to students of his groundbreaking article, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890), which he cowrote with Samuel Warren. Justice Holmes joined Justice Brandeis's decision in *Olmstead*, but wrote separately to emphasize his view—maintained since at least *Silverthorne Lumber Co. v. United States*, 251 U.S. 385 (1920)—that federal courts should not be in the business of sanctioning criminal conduct by law enforcement officers by admitting into evidence the products of illegal conduct. *See Olmstead*, 277 U.S. at 485 (Brandeis, J., dissenting) ("Decency, security and liberty alike demand that government officials shall be subjected to the same rules of conduct that are commands to the citizen. In a government of laws, existence of the government will be imperilled if it fails to observe the law scrupulously. Our Government is the potent, the omnipresent teacher. For good or for ill, it teaches the whole people by its example. Crime is contagious. If the Government becomes a lawbreaker, it breeds contempt for law; it invites every man to become a law unto himself; it invites anarchy. To declare that in the administration of the criminal law, the end justifies the means—to declare that the Government may commit crimes in order to secure the conviction of a private criminal—would bring terrible retribution. Against that pernicious doctrine this Court should resolutely set its face."). For an extended explanation of Justice Holmes's view in the context of the Court's broader exclusionary rule jurisprudence, see Gray, *Spectacular Non Sequitur*, *supra* note 21.

[41] *Olmstead*, 277 U.S. at 473 (Brandeis, J., dissenting).

[42] *Id.*

[43] *Id.* at 474 ("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. Advances in the psychic and related sciences may bring means of exploring unexpressed beliefs, thoughts and emotions. 'That places the liberty of every man in the hands of every petty officer' was said by James Otis of much lesser intrusions than these. To Lord Camden, a far slighter intrusion seemed 'subversive of all the comforts of society.' Can it be that the Constitution affords no protection against such invasions of individual security?") (footnotes omitted).

[44] *Id.* at 478.

on the Fourth Amendment's reach slowly took hold. The Court famously took stock of these shifts in *Katz v. United States*.[45] There, the Federal Bureau of Investigation suspected that Mr. Katz was conducting an illegal bookmaking operation using a public telephone booth.[46] To gather evidence against him, agents attached an electronic listening device to the outside of the booth. Using that "electronic ear," they overheard and recorded incriminating statements that Katz made to his clients and associates, which otherwise would have been kept private within the confines of the booth.

There is no doubt that what the agents did in *Katz* constituted eavesdropping. Given the Court's holding in *Olmstead*, they must nevertheless have been quite confident in the constitutionality of their surveillance.[47] After all, *Olmstead* made clear that, absent a property interest and physical intrusion, the Fourth Amendment imposed no constraints on law enforcement conduct.[48] Because the phone booth in question was a public resource, Katz could not claim any property interest in it. Moreover, even if he could claim a property interest in the booth, the device was attached to the outside of the booth and thus its installation and use did not entail a physical invasion. By application of *modus tollens* to premises set forth by the Court in *Olmstead*, it therefore appeared that the agents' use of an electronic device to listen surreptitiously to and record Mr. Katz's conversations in that booth was not a "search" or "seizure" subject to Fourth Amendment regulation.

Nevertheless, Justice Stewart, writing for the Court, held that Katz's Fourth Amendment rights had been violated. Citing a line of cases since *Olmstead* and the increasing ubiquity of telephone communications,[49] Justice Stewart found that "the underpinnings of *Olmstead* . . . have been so eroded by our subsequent decisions that the 'trespass' doctrine there

---

[45] 389 U.S. 347 (1967).

[46] *Id.* at 354.

[47] *Id.* at 352 ("The Government contends, however, that the activities of its agents in this case should not be tested by Fourth Amendment requirements, for the surveillance technique they employed involved no physical penetration of the telephone booth from which the petitioner placed his calls.").

[48] *Id.* at 352–53 (noting that "a closely divided Court supposed in *Olmstead* that surveillance without any trespass and without the seizure of any material object fell outside the ambit of the Constitution").

[49] *Id.* at 352 ("[A] person in a telephone booth may rely upon the protection of the Fourth Amendment. One who occupies it, shuts the door behind him, and pays the toll that permits him to place a call is surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world. To read the Constitution more narrowly is to ignore the vital role that the public telephone has come to play in private communication.").

enunciated can no longer be regarded as controlling."[50] Rather, he wrote, "the Fourth Amendment protects people, not places."[51] Instead of focusing on an individual's property interests, the Court turned its attention to what Justice Harlan referred to as Katz's "constitutionally protected reasonable expectation of privacy."[52] With those expectations in focus, the Court found that: "What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection . . . . But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[53] Noting that Katz had closed the door of the phone booth with the reasonable expectation that his conversations would not be accessible to the public,[54] the Court held that "[t]he Government's activities in electronically listening to and recording [Katz's] words violated the privacy upon which he justifiably relied while using the telephone booth and thus constituted a 'search and seizure' within the meaning of the Fourth Amendment."[55] "The fact that the electronic device employed to achieve that end did not happen to penetrate the wall of the booth," Justice Stewart concluded, "can have no constitutional significance."[56]

Katz marked a significant shift in Fourth Amendment analysis and doctrine. The threshold questions in any Fourth Amendment case are whether there has been a "search" or a "seizure," and whether the litigant at bar has "standing" to assert a violation. After *Katz*, the answer to both questions has been a function of whether the person alleging a Fourth Amendment violation has subjectively manifested an expectation of privacy that society is prepared to recognize as reasonable.[57] Unsurprisingly, the answer depends on the context. There are, nevertheless, some broad and important rules. For example, the Court has time and again defended as reasonable the expectations of privacy that we have in our homes, persons, and immediate possessions.[58] That is, despite its protestations in *Katz* that "the Fourth Amendment protects people, not places,"[59] much of the Court's

---

[50] *Id.* at 353.

[51] *Id*. at 351.

[52] *Id.* at 360 (Harlan, J., concurring).

[53] *Id.* at 351–52 (majority opinion) (internal citations omitted).

[54] *Id.* at 352 ("The Government stresses the fact that the telephone booth from which the petitioner made his calls was constructed partly of glass, so that he was as visible after he entered it as he would have been if he had remained outside. But what he sought to exclude when he entered the booth was not the intruding eye—it was the uninvited ear.").

[55] *Id.* at 353.

[56] *Id.*

[57] United States v. Jones, 132 S. Ct. 945, 950 (2012).

[58] Kyllo v. United States, 533 U.S. 27, 40 (2001).

[59] 389 U.S. at 351.

post-*Katz* jurisprudence has in one way or another been about charting the social geography of public and private spaces—a journey that often is difficult to navigate.[60] Adding to the difficulties, the territory it has mapped is not composed entirely of mountains and valleys. Rather, we find, there is a range of spaces in between, including cars[61] and businesses,[62] where we enjoy "diminished" expectations of privacy.

The impact of *Katz* on Fourth Amendment law is not limited to assessing these threshold questions of search, seizure, and standing. The Fourth Amendment does not prohibit searches and seizures, after all, but rather prohibits only "unreasonable" searches and seizures. By linking the Fourth Amendment to reasonable expectations of privacy rather than property rights, *Katz* provided a ready analytical structure for evaluating whether a search or seizure is "reasonable" that asks courts to strike a balance between the competing interests of law enforcement and citizens.[63] So, for example, a search conducted under the authority of a warrant issued by a detached and neutral magistrate, based on facts sufficient to provide probable cause to believe that specified evidence will be found in a particular home at an appointed time, is "reasonable" because the combination of grounded suspicion, judicial review, and particularity strikes a reasonable balance between law enforcement interests in detecting and prosecuting crime and the target's reasonable expectations of privacy in his home.[64] This warrant requirement also imposes broad constraints on law enforcement's authority to search our homes generally, thereby guaranteeing a reasonable degree of security for all of us. Similarly, the general requirement that officers "knock and announce" before conducting a warranted search reflects a reasonable balance between law enforcement's interests in self-protection and preserving evidence on the one hand, and the privacy, safety, and property interests of people on the premises at the time on the other.[65]

The general approach of assessing Fourth Amendment search, seizure, standing, and reasonableness by focusing on competing interests of citizens and law enforcement has produced a series of important doctrines. Two are paramount for present purposes: the public-observation doctrine and the third-party doctrine. The public-observation doctrine holds that law

---

[60] *See* Kerr, *Mosaic*, *supra* note 19.

[61] Wyoming v. Houghton, 526 U.S. 295, 300, 305 (1999).

[62] Berger v. New York, 388 U.S. 41, 64 (1967).

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

[64] Johnson v. United States, 333 U.S. 10, 14–15 (1948).

[65] Wilson v. Arkansas, 514 U.S. 927, 934–36 (1995).

enforcement can freely make observations from any place where they lawfully have a right to be.[66] The rationale underlying this rule derives directly from *Katz*, where the Court maintained that we have no reason to expect privacy in activities "knowingly expose[d] to the public."[67] Because observations made from a public place do not implicate citizens' reasonable expectations of privacy, law enforcement officers have unfettered discretion to pursue their interests in detecting and prosecuting crime by any means that is analogous—from a *Katz* point of view—to standing on a street corner. Applying the public-observation doctrine, the Court has held that police may rummage through garbage cans set out for collection,[68] look down into our yards from public airspace,[69] and monitor our comings and goings on public roads,[70] without the need for a warrant or other judicial review. That is because, in theory at least, any member of the public could do the same; therefore, no reasonable expectations of privacy need to be considered.

The third-party doctrine holds, in essence, that the only way to keep a secret is not to tell anyone. It suggests that people should reasonably expect that anytime they share information with a confidant they run the risk that the information will be shared with others. When this occurs, we can complain about breaches of trust by our erstwhile confidants, but not about those with whom the information has been shared. Following similar logic, the Court has ruled that the Fourth Amendment cannot save us from ill-placed trust if those with whom we share private information pass it along to law enforcement.[71] Applying this rule, the Court has held that the Fourth Amendment does not prohibit the government from using lawful means to gain access to privately recorded conversations,[72] "pen registers" of telephone calls kept by telephone companies,[73] or lists of financial transactions kept by financial institutions.[74] Here again, law enforcement's discretion to gather and use information from third parties is not constrained by the Fourth Amendment because there are no competing privacy interests that require accommodation.[75]

---

[66] *See* Florida v. Riley, 488 U.S. 445, 451–52 (1989).

[67] Katz v. United States, 389 U.S. 347, 351 (1967).

[68] California v. Greenwood, 486 U.S. 35, 37 (1988).

[69] California v. Ciraolo, 476 U.S. 207, 213–14 (1986).

[70] United States v. Knotts, 460 U.S. 276, 281–82 (1983).

[71] United States v. White, 401 U.S. 745, 752 (1971).

[72] *Id.* at 749–50.

[73] Smith v. Maryland, 442 U.S. 735, 742 (1979).

[74] California Banker's Ass'n v. Shultz, 416 U.S. 21, 52 (1974).

[75] The limited reach of the Fourth Amendment does not bar the political branches from setting limits on the flow of information from third parties to law enforcement. In fact,

As we shall see in Parts III and IV, the public-observation and the third-party doctrines play a critical role in law enforcement's efforts to detect and prosecute many crimes, particularly cybercrimes. That is important because these doctrines appear to be under threat after the Court's decision in *United States v. Jones*.

In *Jones*, an interagency group of law enforcement officers associated with an FBI–Metropolitan Police Department Task Force was investigating Lawrence Maynard and Antoine Jones on suspicion that they were part of a conspiracy to import, process, and distribute narcotics in and around the District of Columbia.[76] During the course of their investigation, officers obtained warrants to tap Jones's and Maynard's phones as well as a warrant that permitted them to install and monitor a GPS-enabled tracking device on Jones's automobile.[77] Surveillance conducted over the next four weeks using the wiretap and the GPS device was productive, providing investigators with several incriminating statements and over 2,000 pages of information documenting Jones's regular visits to stash houses and other locations tied to the broader drug conspiracy.[78]

At trial, Jones moved to suppress evidence gathered using the GPS-enabled tracking device. His principal argument was that the officers failed to abide by the terms of the warrant.[79] Relying on the public-observation doctrine, the trial court denied Jones's motion. The vast majority of what the GPS device gathered was information documenting Jones's travels over public roads.[80] Because this was information that he knowingly revealed to the public, the court reasoned that Jones lacked a reasonable expectation of privacy. Although the officers had violated the terms of their warrant when installing the GPS device, the court ruled that no warrant was required in the first place because the surveillance conducted using the device did not implicate any of the privacy interests that the warrant requirement is designed to accommodate.[81] That the officers violated the terms of the

---

Congress has passed laws protecting financial information shared with banks, phone records, and even video rental histories. *Existing Federal Privacy Laws*, CTR. FOR DEMOCRACY & TECH., https://www.cdt.org/privacy/guide/protect/laws.php (last visited May 21, 2013). The Fifth, Sixth, and Fourteenth Amendments limit law enforcement's ability to obtain coerced confessions that defendants admitted to third parties. Arizona v. Fulminante, 499 U.S. 279, 288 (1991).

[76] United States v. Jones, 132 S. Ct. 945, 948 (2012).

[77] *Id.*

[78] *Id.*

[79] *Id.* The warrant required that the device be installed within ten days, but it was installed on the eleventh day. The warrant also required that the device be installed within the borders of the District of Columbia, but it was installed in a Maryland parking lot.

[80] *Id.*

[81] *Id.*

warrant was therefore of no constitutional consequence.

The trial court's reasoning in *Jones* was well-grounded in post-*Katz* doctrine, particularly the Supreme Court's decision in *United States v. Knotts*.[82] There, the Court was asked to determine whether law enforcement's use of a radio beeper tracking device to monitor the public movements of a suspect under investigation for alleged participation in a drug conspiracy constituted a "search" for purposes of the Fourth Amendment.[83] Affirming its commitment to the public-observation doctrine, the Court held that it did not.[84] Although the beeper device allowed the officers in *Knotts* to track their suspect over city streets, even after they lost visual contact, the Court found that "scientific enhancement of this sort raises no constitutional issues which visual surveillance would not also raise," which is to say it raises none at all.[85] The factual parallels between the two cases appeared to the trial court in *Jones* to put the question before it on all fours with the holding in *Knotts*.[86] Although the GPS-enabled tracking device used in *Jones* provided more precise information and required less human engagement than the radio beeper device used in *Knotts*, the information revealed was the same: movements knowingly exposed to public view, to which, the court concluded, Jones had no more reasonable claim of privacy than did Knotts.

Based in part on the information generated using the GPS-enabled tracking device, Jones was convicted.[87] He appealed to the United States Court of Appeals for the District of Columbia Circuit, where he found a sympathetic audience for his Fourth Amendment concerns.[88] Writing for a three-judge panel, Judge Ginsburg focused not on the nature of the GPS surveillance, or the precise type of information gathered at any given moment, but instead on the length of the surveillance and the quantity of information gathered by law enforcement using the GPS-enabled tracking device.[89] Distinguishing *Knotts*, Judge Ginsburg explained that "a person traveling in an automobile on public thoroughfares [may have] no

---

[82] 460 U.S. 276 (1983).

[83] *Id.* at 277.

[84] *Id.* at 285 ("We thus return to the question posed at the beginning of our inquiry in discussing *Katz*, *supra*; did monitoring the beeper signals complained of by respondent invade any legitimate expectation of privacy on his part? For the reasons previously stated, we hold it did not. Since it did not, there was neither a 'search' nor a 'seizure' within the contemplation of the Fourth Amendment.").

[85] *Id.* at 285.

[86] *Jones*, 132 S. Ct. at 948.

[87] *Id.* at 949.

[88] *Id.*

[89] United States v. Maynard, 615 F.3d 544, 556 (D.C. Cir. 2010).

reasonable expectation of privacy in his movements from one place to another," but that does not mean that he "has no reasonable expectation of privacy in his movements whatsoever, world without end."[90] Rather, the court argued, he retains a reasonable expectation of privacy in the whole of his movements over an extended period of time to the extent that the aggregate of those moments reveals "an intimate picture of his life."[91]

Drawing specific links to the *Katz* framework, Judge Ginsburg argued that "the whole of one's movements over the course of a month is not *actually* exposed to the public because the likelihood anyone will observe all those movements is effectively nil."[92] Relying on this "mosaic theory" of Fourth Amendment privacy, the circuit court therefore held that Jones had a "[reasonable] expectation of privacy in his movements over the course of a month," even if he had no such expectation of privacy in the constitutive particulars.[93] Because the officers who installed and monitored the GPS device gathered information on Jones's movements for nearly a month, and without lawful authority of a warrant issued on probable cause by a detached and neutral magistrate, the court vacated Jones's conviction.

Much to the surprise of many Court watchers, the Supreme Court affirmed.[94] Writing for a five-Justice majority, Justice Scalia deferred consideration of the circuit court's mosaic theory[95] and focused instead on the installation of the GPS device on Jones's car. In the majority's view, merely installing the device constituted a search under the Fourth Amendment, not because it violated subjectively manifested expectations of

---

[90] *Id.* at 557.

[91] *Id.* at 562; *see also id.* at 562 ("The difference is not one of degree, but of kind, for no single journey reveals the habits and patterns that mark the distinction between a day in the life and a way of life, nor the departure from a routine that, like the dog that did not bark in the Sherlock Holmes story, may reveal even more."); *id.* at 563 ("[P]rolonged GPS monitoring reveals an intimate picture of the subject's life that he expects no one to have—short perhaps of his spouse.").

[92] *Id.* at 558; *see also id.* at 563 ("A reasonable person does not expect anyone to monitor and retain a record of every time he drives his car, including his origin, route, destination, and each place he stops and how long he stays there; rather, he expects each of those movements to remain 'disconnected and anonymous.'") (citation omitted). In an analogous way, state harassment laws and privacy tort law have reinforced the notion that people can expect to be free from unreasonable surveillance. *See, e.g.*, Galella v. Onassis, 487 F.2d 986, 998–99 (2d Cir. 1973) (upholding injunction of a persistent paparazzo); Wolfson v. Lewis, 924 F. Supp. 1413, 1420, 1433–34 (E.D. Pa. 1996) (enjoining surveillance of a family on the grounds it was part of "a persistent course of hounding, harassment and unreasonable surveillance, even if conducted in a public or semi-public place").

[93] *Maynard*, 615 F.3d at 563.

[94] United States v. Jones, 132 S. Ct. 945, 954 (2012).

[95] *Id.* ("We may have to grapple with these 'vexing problems' in some future case where a classic trespassory search is not involved and resort must be had to *Katz* analysis; but there is no reason for rushing forward to resolve them here.").

privacy that society is prepared to recognize as reasonable, but because it entailed a trespass for the purpose of obtaining information.[96] Surveying major Fourth Amendment cases since *Katz*, Justice Scalia found the reported death of the trespass principles underlying *Olmstead*[97] were exaggerated.[98] Rather than displacing the traditional trespass approach to the Fourth Amendment, Justice Scalia found that the *Katz* reasonable-expectation-of-privacy test was an edifice built upon common law foundations.[99] Although it was necessary to appeal to those additional protections in *Katz*, and to chart the limits of those extensions in cases like *Knotts*, the facts before the Court in *Jones* simply did not require anything more than a trespass analysis.[100] Because the officers trespassed upon Jones's property for the purpose of obtaining information, the Court held that they engaged in a search.[101] Because that search was neither authorized by a warrant nor otherwise justified by established standards of Fourth Amendment reasonableness, the majority sustained the circuit court's judgment, if not its holding.[102]

The *Jones* majority's revitalization of the trespass approach to defining Fourth Amendment search and seizure was headline-worthy by itself, but the front-page stories came from the two concurring opinions, which together represent the views of a voting majority of five Justices.

Although she joined the majority, Justice Sotomayor wrote a separate concurrence in *Jones* to express her broad sympathies for the privacy interests that would be afforded Fourth Amendment protection by the circuit court's mosaic theory.[103] As she explained, long-term GPS monitoring, such as was conducted in *Jones*, "generates a precise,

---

[96] *Id.*; *see also* United States v. Knotts, 460 U.S. 276, 286 (1983) (Brennan, J., concurring) ("[W]hen the Government *does* engage in physical intrusion of a constitutionally protected area in order to obtain information, that intrusion may constitute a violation of the Fourth Amendment . . . ."). Judge Kavanaugh proposed trespass as a narrower ground for decision in his dissent from the circuit court's denial of the petition for rehearing en banc. *See* United States v. Jones, 625 F.3d 766, 769–71 (2010) (Kavanaugh, J., dissenting).

[97] United States v. Katz, 389 U.S. 347, 353 (1967) ("We conclude that the underpinnings of *Olmstead* . . . have been so eroded by our subsequent decisions that the 'trespass' doctrine there enunciated can no longer be regarded as controlling.").

[98] *Jones*, 132 S. Ct. at 949–54. We allude here to Mark Twain's famous comments on newspaper reports of his death.

[99] *Id.* at 952 ("[T]he *Katz* reasonable-expectation-of-privacy test has been *added to*, not *substituted for*, the common-law trespassory test.").

[100] *Id.* at 954.

[101] *Id.* at 949 ("The Government physically occupied private property for the purpose of obtaining information. We have no doubt that such a physical intrusion would have been considered a 'search' within the meaning of the Fourth Amendment when it was adopted.").

[102] *Id.* at 954.

[103] *Id.* at 954–56 (Sotomayor, J., concurring).

comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations."[104] In addition to its power, Justice Sotomayor noted that GPS monitoring comes "at a relatively low cost," and that leaving the Government with "unfettered discretion" to track whomever it chooses is a recipe for abuse.[105] Under such a regime of constant surveillance, Justice Sotomayor worried that the reality, or the threat, "that the Government may be watching [would] chill[] associational and expressive freedoms," and "alter the relationship between citizen and government in a way that is inimical to democratic society."[106]

Justice Sotomayor acknowledged, as did the circuit court, that adopting the mosaic theory would require abandoning or modifying the public-observation doctrine.[107] She went further, however, by suggesting that implementing the mosaic theory might also require the Court to "reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties."[108] According to Justice Sotomayor, the third-party doctrine "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."[109] In particular, "[p]eople disclose the phone numbers that they dial or text to their cellular providers; the URLs that they visit and the e-mail addresses with which they correspond to their Internet service providers; and the books, groceries, and medications they purchase to online retailers."[110] Attaching her concerns to the *Katz* framework, Justice Sotomayor concluded:

> I for one doubt that people would accept without complaint the warrantless disclosure to the Government of a list of every Web site they had visited in the last week, or month, or year. But whatever the societal expectations, they can attain constitutionally protected status only if our *Fourth Amendment* jurisprudence ceases to treat secrecy as a prerequisite for privacy.[111]

In a separate concurring opinion joined by Justices Ginsburg, Breyer, and Kagan, Justice Alito also expressed significant sympathy for the circuit court's mosaic theory of Fourth Amendment privacy.[112] Like Justice Sotomayor, Justice Alito simply could not see why the public-observation

---

[104] *Id.* at 955.
[105] *Id.* at 956.
[106] *Id.*
[107] *Id.*
[108] *Id.* at 957.
[109] *Id.*
[110] *Id.*
[111] *Id.*
[112] *Id.* at 963–64 (Alito, J., concurring in the judgment).

doctrine should survive without significant modification given the government's dramatically expanded surveillance capacities. "In the pre-computer age," he notes, "the greatest protections of privacy were neither constitutional nor statutory, but practical."[113] It was nearly impossible, or at least prohibitively expensive, for law enforcement to engage in the kind of continuous, long-term surveillance to which Jones was subjected.[114] We could therefore rest assured that the government was not watching all of us constantly, or even very many of us at any given time.[115] Justice Alito therefore would have held that "short-term monitoring of a person's movements on public streets accords with expectations of privacy that our society has recognized as reasonable," but that "longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy."[116]

Together, the concurring opinions in *Jones* represent a majority of sitting Justices who appear to be willing to adopt some version of the mosaic theory of Fourth Amendment privacy. Doing so would, as these Justices recognize, require abandoning or modifying both the public-observation doctrine and the third-party doctrine.[117] This possibility has sent tremors through the community of those interested in Fourth Amendment issues, including law enforcement officers. That is because many widely used, and often critical, investigative technologies, methods, and strategies that have until now operated outside of Fourth Amendment regulations may soon be subject to Fourth Amendment controls. Although the Fourth Amendment would not necessarily bar GPS tracking and other surveillance technologies, methods, and strategies that implicate reasonable expectations of privacy in informational mosaics, it will impose limits on their use by requiring courts to balance the competing interests of law enforcement in detecting and prosecuting crime, and citizens' interests in privacy.[118] As we look towards that future, it is important to have a clear

---

[113] *Id.* at 963.

[114] *Id.* at 964; *see also* Renée McDonald Hutchins, *Tied Up in* Knotts*? GPS Technology and the Fourth Amendment*, 55 UCLA L. REV. 409, 455–56 (2007).

[115] *Jones*, 132 S. Ct. at 963–64 (Alito, J., concurring in the judgment); *see also* Hutchins, *supra* note 114, at 455–56.

[116] *Jones*, 132 S. Ct. at 964 (Alito, J., concurring in the judgment); *see also* Stephen E. Henderson, *Nothing New Under the Sun? A Technologically Rational Doctrine of Fourth Amendment Search*, 56 MERCER L. REV. 507, 547–48 (2005).

[117] *Jones*, 132 S. Ct. at 957 (Sotomayor, J., concurring); *id.* at 964 (Alito, J., concurring in the judgment).

[118] *Id.* at 964 (Alito, J., concurring in the judgment) (arguing that long-term use of GPS-enabled tracking technology would require a warrant issued by a detached and neutral magistrate based upon probable cause); Jason M. Weinstein, *Public Safety and Online Privacy—Myth Versus Reality*, 11 NW. J. TECH. & INTELL. PROP. 33, 38–39 (2013).

understanding of what those competing interests are. The *Jones* concurrences, and their cadres of supporters, have done a great deal to focus attention on the privacy interests that would sit on one side of that scale.[119] The counterbalancing governmental interests at stake have received far less attention, however. This is particularly true for many cybercrimes, which are relatively new, increasingly complex, and often unfamiliar to citizens who have not been victims. In the next two Parts, we begin to remedy that omission by highlighting the significant law enforcement interests at stake in healthcare fraud and cyberharassment.

III. THE GOVERNMENT'S LEGITIMATE INTERESTS IN PREVENTING, DETECTING, AND PROSECUTING HEALTHCARE FRAUD

Should the Court eventually hold that citizens have reasonable expectations of privacy in mosaics of personal information, it will then need to provide some guidance to law enforcement, legislatures, and lower courts on the impact of the mosaic theory on the Court's core Fourth Amendment balancing test and on well-settled doctrinal rules like the public-observation doctrine and the third-party doctrine. In this Part, we explore the role that investigative techniques and technologies that are likely to trigger mosaic theory concerns play in advancing legitimate governmental interests in preventing, detecting, and prosecuting healthcare fraud.

A. BIG DATA AND THE MOSAIC THEORY

Data-collection capabilities are increasing at an unprecedented rate.[120] Not surprisingly, government agencies that investigate criminal offenses seek as much access to data as possible. Cell phone carriers recently reported that law enforcement agencies from all levels of government submitted at least 1.3 million requests for user data in 2011.[121] Some of the carriers are so overwhelmed by such requests that they are outsourcing the responses to third parties.[122] In March 2012, journalist James Bamford, relying on anonymous governmental sources, reported that NSA was building a massive data-collection and storage center in Utah.[123] According

---

[119] We are certainly among them. *See* Gray & Citron, *Quantitative Privacy*, *supra* note 7.

[120] *See* Danielle Keats Citron, *Reservoirs of Danger: The Evolution of Public and Private Law at the Dawn of the Information Age*, 80 S. CAL. L. REV. 241, 246–47 (2007) (describing the recent advances and comparing to past rate of growth).

[121] Eric Lichtblau, *More Demands on Cell Carriers in Surveillance*, N.Y. TIMES, July 9, 2012, at A1.

[122] *Id.* ("The outside provider, Neustar, said it handled law enforcement compliance for about 400 phone and Internet companies.").

[123] James Bamford, *The NSA Is Building the Country's Biggest Spy Center (Watch What*

to Bamford:

> Flowing through its servers and routers and stored in near-bottomless databases will be all forms of communication, including the complete contents of private emails, cell phone calls, and Google searches, as well as all sorts of personal data trails—parking receipts, travel itineraries, bookstore purchases, and other digital "pocket litter."[124]

NSA is not alone. Around the same time the Utah center was raising concerns, the National Counterterrorism Center (NCTC) obtained discretionary access to nearly all data collected by the federal government, including, but not limited to, information on "every airline passenger entering the U.S.," federally backed mortgage recipients' financial data, and Veterans Affairs medical records.[125] NCTC hopes to analyze the data in order to detect patterns that indicate terrorist activity.[126]

As these programs show, the federal government collects and analyzes sizable amounts of data for a variety of purposes, from the administration of public benefits to the administration of the census. Healthcare-related data is a prominent part of the mix. For example, the Patient Protection and Affordable Care Act (ACA) requires "any federally conducted or supported health care or public health program, activity or survey (including Current Population Surveys and American Community Surveys conducted by the Bureau of Labor Statistics and the Bureau of the Census) [to] collect[] and report [to Health and Human Services (DHHS)], to the extent practicable" patient-reported information on sex, race, ethnicity, language, disability, gender identity, and sexual orientation.[127] DHHS will, in turn, aggregate and analyze "quality and resource use measures from information systems used to support health care delivery"[128] and release to qualified private or public entities "standardized extracts" of Medicare Part A, B, and D claims

---

You Say), WIRED (Mar. 15, 2012, 7:24 PM), http://www.wired.com/threatlevel/2012/03/ff_nsadatacenter/.

[124] *Id.* Bamford concluded that the new Utah center would be "the realization of the 'total information awareness' program." *Id.* Bamford's accusations prompted a congressional investigation and interview of NSA's chief, who denied the accusations, but Bamford points to both insider information and unique NSA definitions of words like "intercept" to support his original report. James Bamford, *NSA Chief Denies Domestic Spying but Whistleblowers Say Otherwise*, WIRED (Mar. 21, 2012, 2:37 PM), http://www.wired.com/threatlevel/2012/03/nsa-whistleblower/all/.

[125] Julia Angwin, *U.S. Terror Agency to Tap Citizen Files*, WALL ST. J., Dec. 13, 2012, at A1.

[126] Charlie Savage, *U.S. Eases Rule on Use of Data on Americans*, N.Y. TIMES, Mar. 23, 2012, at A1 ("Moreover, the first two tracks for searching the databases that remain under the control of the original agencies prohibit 'pattern analysis.' But that restriction does not apply to databases the center has copied.").

[127] The Patient Protection and Affordable Care Act, Pub. L. No. 111-148, § 3101, 124 Stat. 119, 578 (2010).

[128] *Id.* § 10305, 124 Stat. at 939.

for purposes of "performance measurement."[129] Pursuant to the ACA, DHHS is authorized to expand the types of information it collects.[130]

Outside the provisions of the ACA, DHHS and Medicare programs also collect data from contracted intermediaries, such as the private insurance companies that manage claim reviews, and from Quality Improvement Organizations (QIOs), which are typically private nonprofits.[131] In addition to supplying data, QIOs assist providers who participate in the Electronic Record Health Incentive Program, which requires reporting clinical quality measures like "health outcomes, clinical processes, patient safety, efficient use of healthcare resources, care coordination, patient engagements, population and public health, and clinical guidelines."[132] Hospitals also provide the Centers for Medicare and Medicaid Services (CMS) with patient survey information, readmission statistics, and nosocomial infection data.[133] More recently, DHHS announced a data-sharing partnership with the nation's leading private insurance providers.[134]

The amount of personal information, including health information, aggregated by government agencies, is referred to as "Big Data," and for good reason. Federal agencies, state authorities, and their private contractors store mind-boggling amounts of information. Given the quantity and scope of this information, there can be no doubt that Big Data implicates privacy interests recognized by the mosaic theory of Fourth Amendment privacy endorsed to varying degrees by the concurring opinions in *Jones*.[135] As the mosaic theory suggests, aggregations of rather

---

[129] *Id.* § 10332, 124 Stat. at 968. The Secretary of HHS determines the format of the released data and is responsible for protecting beneficiary privacy. *Id.*

[130] *Id.* § 6504, 124 Stat. at 776–77 (adding "data elements from the automated data system that the Secretary determines to be necessary for program integrity, program oversight, and administration, at such frequency as the Secretary shall determine" to the information a State must provide to receive reimbursement for maintaining automated data systems under 42 U.S.C. § 1396b (2006)).

[131] *Quality Improvement Organizations*, CTRS. FOR MEDICARE & MEDICAID SERVS., http://www.cms.gov/Medicare/Quality-Initiatives-Patient-Assessment-Instruments/QualityImprovementOrgs/index.html (last modified May 20, 2013).

[132] *Clinical Quality Measures*, CTRS. FOR MEDICARE & MEDICAID SERVS., http://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/ClinicalQualityMeasures.html (last modified Apr. 4, 2013).

[133] *Data Sources*, MEDICARE.GOV, http://www.medicare.gov/HospitalCompare/Data/AboutData/Data-Sources.aspx (last visited May 25, 2013).

[134] Press Release, Dep't of Health and Human Servs., Obama Administration Announces Ground-Breaking Public-Private Partnership to Prevent Health Care Fraud (July 26, 2012), *available at* http://www.hhs.gov/news/press/2012pres/07/20120726a.html.

[135] *See, e.g.*, Danielle Citron, *Big Data Brokers as Fiduciaries*, CONCURRING OPINIONS (June 19, 2012, 5:08 PM), http://www.concurringopinions.com/archives/2012/06/big-data-

innocuous information may "reveal[] more—sometimes a great deal more—than does the sum of its parts."[136] This is a particularly likely prospect given Big Data's use of increasingly sophisticated analytics, which promise to reveal far more about us than is disclosed by the raw bits and bytes, no matter how "big" or small the data.[137] The dangers are yet more pronounced if health-related data is part of the mix because of what this information can reveal about the most intimate of our affairs.[138]

Healthcare data, by definition, contains information that the Supreme Court has already ruled fundamentally private, such as reproductive choice,[139] and information that the Court may deem private in the near future, such as genetic data.[140] But not all healthcare data is protected. In *Whalen v. Roe*, the Court found no threat to privacy in a law that required physicians to report to the Department of Health personal and identifying information of patients who were prescribed certain drugs.[141] Because the required disclosure was similar to existing and essential procedures, like mandatory child abuse reporting or sharing information with insurance companies for reimbursement,[142] and the statute provided adequate security against data breach, the Court held that any risk to patient privacy was

---

brokers-as-fiduciaries.html (describing some of the dangers of Big Data for citizens).

[136] United States v. Maynard, 615 F.3d 544, 558 (D.C. Cir. 2010).

[137] *See* Charles Duhigg, *How Companies Learn Your Secrets*, N.Y. TIMES (Feb. 16, 2012), http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html?pagewanted=all&_r=0 (recounting how Target uses publicly available databases and market analytics to identify women who are in the early stages of pregnancy).

[138] *Cf.* United States v. Jones, 132 S. Ct. 945, 955–56 (2012) (Sotomayor, J., concurring) (pointing out how GPS-enabled surveillance is capable of painting detailed pictures of subjects' private lives when they reveal information such as "'trips to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center'" (quoting People v. Weaver, 909 N.E.2d 1195, 1199 (N.Y. 2009))).

[139] *See, e.g.*, Griswold v. Connecticut, 381 U.S. 479, 485–86 (1965) (holding that a law forbidding contraception was an unacceptable invasion of marital privacy). In criticizing the contraception law, the *Griswold* Court touched on the issue of police investigation, remarking, "Would we allow the police to search the sacred precincts of marital bedrooms for telltale signs of the use of contraceptives? The very idea is repulsive to the notions of privacy surrounding the marriage relationship." *Id.*

[140] *See, e.g.*, David Kravets, *Pivotal DNA Privacy Case Gets Supreme Court Hearing*, WIRED (Nov. 9, 2012, 4:57 PM), http://www.wired.com/threatlevel/2012/11/scotus-grants-dna-case/ (reporting that the Court has decided to hear *King v. State*, 42 A.3d 549 (Md. 2012), *cert. granted*, 133 S. Ct. 594 (2012), a case in which the suspect was required to give a DNA sample upon arrest, which later led to a conviction for another crime).

[141] Whalen v. Roe, 429 U.S. 589, 603–04 (1977). The reporting form included the name of "the prescribing physician; the dispensing pharmacy; the drug and dosage; and the name, address, and age of the patient." *Id.* at 593.

[142] *Id.* at 602 & n.29.

insufficient to violate the Fourteenth Amendment.[143] In so holding, however, the Court hinted that, absent adequate security measures, government acquisition or disclosure of massive amounts of private data would implicate privacy protections.[144] In his concurrence, Justice Brennan did more than hint, suggesting that it may be necessary to restrain technological advancements that make such data accumulations possible.[145]

A little over ten years later, the Court again considered privacy issues relating to data aggregation, this time in the form of rap sheets.[146] Although the individual criminal events that compose a rap sheet may be public record, the Court held that the rap sheet, as a summary of the total criminal events in an individual's life, represented a potential and "substantial"[147] threat to privacy,[148] particularly because of advances in technology that allowed for greater storage capacity.[149] Unlike in *Whalen*, where the Court emphasized the routine disclosure of confidential information under specific but frequent circumstances, the Court in *U.S. Department of Justice v. Reporters Committee for Freedom of the Press* took pains to illustrate the very limited and considered means by which a third party can access rap sheet data.[150] Additionally, the Court dismissed the argument that the

---

[143] *Id.* at 603–04. The Court also refused to find any violation of privacy under the Fourth Amendment because, the cases cited, unlike in *Whalen*, "involve[d] affirmative, unannounced, narrowly focused intrusions into individual privacy during the course of criminal investigations." *Id.* at 604 n.32.

[144] *Id.* at 605–06.

[145] *Id.* at 606–07 (Brennan, J., concurring).

[146] U.S. Dep't of Justice v. Reporters Comm. for Freedom of the Press, 489 U.S. 749, 752 (1989) ("Rap sheets compiled pursuant to such authority contain certain descriptive information, such as date of birth and physical characteristics, as well as a history of arrests, charges, convictions, and incarcerations of the subject. . . . [T]hey are sometimes incorrect or incomplete and sometimes contain information about other persons with similar names.").

[147] *Id.* at 771.

[148] *See id.* at 764 ("Plainly there is a vast difference between the public records that might be found after a diligent search of courthouse files, county archives, and local police stations throughout the country and a computerized summary located in a single clearinghouse of information.").

[149] *Id.* at 771 ("The substantial character of that interest is affected by the fact that in today's society the computer can accumulate and store information that would otherwise have surely been forgotten long before a person attains age 80, when the FBI's rap sheets are discarded."). The Court also quoted heavily from the dissent of the District of Columbia Circuit Court of Appeals decision, which warned against turning the government into a "clearinghouse for highly personal information." *Id.* at 761 (quoting Reporters Comm. for Freedom of the Press v. U.S. Dep't of Justice, 831 F.2d 1124, 1130 (D.C. Cir. 1987) (Starr, J., dissenting), *rev'd*, 489 U.S. 749 (1989)).

[150] *Id.* at 752 (explaining that the FBI considers rap sheets "confidential and, with certain exceptions, has restricted their use to governmental purposes"); *id.* at 753 (describing the three exceptions Congress created for the release of rap sheets: (1) as required by State licensing requirements; (2) "to self-regulatory organizations in the securities industry," and

privacy interest in the sum of public events listed on a rap sheet "approaches zero."[151] The Court concluded that "although there is undoubtedly some public interest in anyone's criminal history," the interest is not central to the government-monitoring purpose of FOIA, which is to allow citizens to monitor the government, not individuals.[152]

Although neither of these cases implicated the Fourth Amendment, they involved personal data similar or identical to that which is currently being collected and stored as part of Big Data projects. Accordingly, they incorporate key factors the Court may use to decide whether large quantities of aggregated healthcare data can trigger privacy concerns. Among these seem to be the extent to which disclosure is commonplace, whether the data is aggregated or dispersed, and the intent of the law authorizing collection or release. The last factor is crucial as it relates to Big Data. The stated intent of the ACA is quite broad, ranging from quality control to fraud prevention to cost containment.[153] By giving researchers, law enforcement, and administrators access to large amounts of information, Big Data could conceivably be used for all three purposes and more.

As we pointed out in Part II, the fact that contemporary surveillance technology, including data-aggregation technology and sophisticated analytics deployed as part of "Big Data," may constitute a Fourth Amendment "search" does not mean that the government and its agents should be denied all access. Rather, what the Fourth Amendment demands is a balancing of legitimate governmental interests served by Big Data with the privacy interests threatened by Big Data. To this point, most of the academic articles and journalistic exposés on Big Data have focused on the second half of that equation. In the remainder of this Part, we draw attention to one important weight on the government's side of the scale: efforts to prevent, detect, and prosecute healthcare fraud.

B. THE VALUE OF BIG DATA IN COMBATING HEALTHCARE FRAUD

Any reasonable discussion of healthcare fraud must include Medicare. Medicare is a government health insurance program for the elderly and the disabled.[154] Every day, 4.5 million claims for Medicare services are

(3) for "licensees or applicants before the Nuclear Regulatory Commission").

[151] *Id.* at 763.

[152] *Id.* at 774.

[153] *See, e.g.*, Patient Protection and Affordable Care Act, Pub. L. No. 111-148, §§ 1313, 3001, 124 Stat 119, 184, 353 (2010).

[154] *What Is Medicare?*, MEDICARE.GOV, http://www.medicare.gov/sign-up-change-plans/decide-how-to-get-medicare/whats-medicare/what-is-medicare.html (last visited May 21, 2013).

processed.[155] In 2011, the program covered almost 49 million people, spending over $500 billion.[156] The extent of Medicare fraud is unknown,[157] but it is believed to cost the government somewhere between $60 billion and $90 billion a year.[158] Hospitalization claims are the most common source of civil fraud investigations, while outpatient, medical equipment, and lab work claims are the most common sources of criminal fraud investigations.[159] Home-health agencies and providers of durable medical equipment have particularly high fraud rates.[160]

Healthcare fraud generally—and Medicare fraud in particular—frequently involves health providers' charging for services never provided, billing for unnecessary equipment, stealing medical identities, paying kickbacks for referrals, or using a Medicare number for fraudulent billing. Complex schemes often incorporate a mix of strategies.[161] To identify

---

[155] CTRS. FOR MEDICARE AND MEDICAID SERVS., DEP'T OF HEALTH & HUMAN SERVS., REPORT TO CONGRESS: FRAUD PREVENTION SYSTEM—FIRST IMPLEMENTATION YEAR 11 (2012), *available at* http://www.stopmedicarefraud.gov/fraud-rtc12142012.pdf; *Medicare Advantage Plans*, MEDICARE.GOV., http://www.medicare.gov/sign-up-change-plans/medicare-health-plans/medicare-advantage-plans/medicare-advantage-plans.html (last visited May 21, 2013); *What Is Medicare?*, *supra* note 154 (explaining that Part C is the Medicare Advantage Program, which is a managed care system for individuals with both Part A and Part B; Part D is the optional prescription program).

[156] *How Is Medicare Funded?*, MEDICARE.GOV, http://www.medicare.gov/about-us/how-medicare-is-funded/medicare-funding.html (last visited May 21, 2013). With an enrollment of about sixty million people, Medicaid covers more individuals, yet Medicare expenditures were over $150 billion more than Medicaid expenditures. *Medicaid Information by Topic*, MEDICAID.GOV, http://www.medicaid.gov/Medicaid-CHIP-Program-Information/By-Topics/By-Topic.html (last visited May 21, 2013); *NHE Fact Sheet*, CTRS. FOR MEDICARE & MEDICAID SERVS., http://www.cms.gov/Research-Statistics-Data-and-Systems/Statistics-Trends-and-Reports/NationalHealthExpendData/NHE-Fact-Sheet.html (last modified Jan. 9, 2013).

[157] U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-13-213T, TYPES OF PROVIDERS INVOLVED IN MEDICARE CASES, AND CMS EFFORTS TO REDUCE FRAUD 1 (2012) (testimony of Kathleen M. King, Director, Health Care, before the H. Subcomm. on Health, Comm. on Energy & Commerce) [hereinafter GAO-13-213T].

[158] Kennedy, *supra* note 15.

[159] GAO-13-213T, *supra* note 157, at 3–5 (2012) ("According to 2010 data, about one-quarter of the 7,848 subjects investigated in criminal health care fraud cases were medical facilities or were affiliated with these facilities. Additionally, about 16 percent of subjects were durable medical equipment suppliers. . . . Hospitals constituted nearly 20 percent of the 2,339 subjects of civil fraud cases investigated in 2010, and other medical facilities accounted for about 18 percent of the subjects.").

[160] U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-12-801T, MEDICARE: PROGRESS MADE TO DETER FRAUD, BUT MORE COULD BE DONE 4 (2012) (testimony of Kathleen M. King, Director, Health Care, before the H. Subcomm. on Oversight and Investigations, Comm. on Energy & Commerce) (illustrating the weaknesses; GAO successfully created two fake DME providers).

[161] M.B. Pell, *AJC Investigation: Mailbox Medical Schemes on Rise: Medicare Fraud*

fraudulent billing practices, automated systems help investigators flag impossible claims, such as a provider's alleged removal of twenty toenails from three toes or bills for more therapy sessions than Newtonian physics would allow.[162] Phantom billing may involve elaborate schemes in which there are in fact no physical clinics, patients, or health practitioners. For example, a member of an Armenian organized crime group recently admitted to creating a network of clinics and providers that existed only on paper, but nevertheless billed Medicare for nearly $100 million and received over $35 million in payments.[163]

Similar to phantom billing is billing for services that are not medically necessary. In one case, a doctor with a penchant for Playboy models and Picassos received "$1.2 million from Medicare in 2008 . . . a large portion of it from physical therapy," consisting of "heat packs, massage, electrical stimulation and ultrasound."[164] Although government-funded massages are relatively harmless to patients, other unnecessary treatments can be invasive and life threatening. In a recent case, investigators discovered that patients who were disoriented and unable to control their bodily functions were being forced to attend group therapy that served no medical purpose.[165]

Costs Taxpayers, but Agency Claims It's Hard to Stop, ATLANTA J.-CONST., Dec. 2, 2012, at A1 (examining the process scammers use to steal providers' identities and set up phony clinics with post office boxes); Press Release, U.S. Attorney's Office, E. Dist. of Cal., Third Physician Sentenced to Lengthy Prison Sentence in Medicare Fraud Case (Oct. 24, 2012), *available at* http://www.justice.gov/usao/cae/news/docs/2012/10-2012/10-24-12Prakash Sent.html (highlighting a medical office that paid beneficiaries to use their Medicare numbers to bill for phantom services where "[f]ew of these tests were ever performed, none were performed based on any medical need, and clinic employees filled out other portions of the charts using preprinted templates" and "[s]ome clinic employees admitted to performing various tests on themselves, and placing the results in patient files").

[162] Mark Schoofs & Maurice Tamman, *Confidentiality Cloaks Medicare Abuse*, WALL ST. J., Dec. 22, 2010, at A1 ("A physical therapist in Brooklyn . . . billed for so much therapy—more than $2.5 million in 2008 alone—that it would have been virtually impossible for him to have performed it all within state and Medicare guidelines . . . ."); *see also* Frank Pasquale, Grand Bargains for Big Data: The Emerging Law of Health Information 48, 52 (unpublished manuscript) (on file with authors) (explaining that a doctor's billing specialists would "upcode" by billing for time not spent directly with the patient, resulting in daily billings that exceeded 24 hours).

[163] Press Release, U.S. Attorney's Office, S. Dist. of N.Y., Leader of $100 Million Medicare Fraud Scheme Pleads Guilty in Manhattan Federal Court to Racketeering and Other Crimes (Oct. 26, 2012), *available at* http://www.justice.gov/usao/nys/pressreleases/October12/MirzoyanDavitPleaPR.php.

[164] Schoofs & Tamman, *supra* note 162 (explaining that, despite the unusually limited scope of his treatments, a doctor's Medicare earnings were "more than 24 times the Medicare income of the average family doctor, according to a Wall Street Journal analysis of Medicare-claims data" and that he closed his practice after Medicare began denying his claims and worked at a pain management clinic at the time the article was published).

[165] Warren Richey, *US Agents Make Arrests in Massive Medicare Fraud Case in*

Providers altered their records so it would appear that patients benefited from therapy that was anything but helpful.[166] In another case, the government alleged that a nursing home required therapists to use the most expensive treatments on residents, even if the interventions were inappropriate or dangerous.[167] For example, it alleged that a ninety-two-year-old cancer patient in Orlando, who was routinely spitting up blood, nonetheless received 48 minutes of physical therapy, 47 minutes of occupational therapy, and 30 minutes of speech therapy, two days before his death. The day he died, the patient received 35 minutes of physical therapy and was scheduled for more therapy later in the day.[168] CMS reported a dermatologist who, in addition to unnecessarily removing "benign skin lesions," reused sutures, thereby exposing patients to HIV, hepatitis C, and other diseases.[169]

Claims for medical equipment are another common target for fraudsters. Two Los Angeles pastors recently were found guilty of running separate schemes involving power wheelchairs. In the first, the conspirators purchased fraudulent medical documentation and billed Medicare $6,000 for power wheelchairs that actually cost $900.[170] The conspirators also offered wheelchairs and other unnecessary equipment to Medicare beneficiaries in exchange for their Medicare numbers.[171] If Medicare refused to pay for the chairs, the pastor instructed his employees to take the chairs away from the beneficiaries.[172] The funds from the scheme were diverted among sham supply companies run by the pastor's wife and other church members.[173] A second pastor and a doctor who

---

Florida, CHRISTIAN SCI. MONITOR, Oct. 21, 2010, at 8 ("'Employees who failed to cooperate or participate in the fraud were terminated,' the [court] documents say. 'One ATC employee was fired after she discharged several beneficiaries she felt were not eligible . . . due to their mental state.' The records say a senior manager later readmitted those same beneficiaries."). The owner of the company is currently serving a 50-year sentence, "the stiffest Medicare-fraud punishment in history." Jay Weaver, *Women Convicted of Medicare Fraud at Fort Lauderdale Therapy Clinic*, MIAMI HERALD (Nov. 20, 2012), http://www.miamiherald.com/2012/11/19/3105498/women-convicted-of-medicare-fraud.html.

[166] Richey *supra* note 165; Weaver, *supra* note 165.

[167] Thomas M. Burton, *Medicare Fraud Is Charged*, WALL ST. J. (Dec. 3, 2012, 7:26 PM), http://online.wsj.com/article/SB10001424127887323717004578157640024945594.html.

[168] *Id.*

[169] *Medicare Advantage Plans*, *supra* note 155, at 33.

[170] Press Release, U.S. Dep't of Justice, Office of Pub. Affairs, Los Angeles Church Pastor Sentenced to Serve 36 Months in Prison for $14.2 Million Medicare Fraud Scheme (Feb. 27, 2012), *available at* http://www.justice.gov/opa/pr/2012/February/12-crm-256.html.

[171] *Id.*

[172] *Id.*

[173] *Id.*

provided fraudulent documentation pleaded guilty to running a similar conspiracy later in the same year.[174]

Prescription medicines provide another rich territory for healthcare fraud. A well-known dialysis provider was accused in 2012 of intentionally wasting medication by giving multiple partial doses, instead of smaller numbers of full doses, in order to inflate charges.[175] Later that same year, a Miami pharmacy owner pleaded guilty to fraud charges for instructing his employees to retrieve from assisted-living facilities unused medication already billed to Medicare and Medicaid so that it could be repackaged and reused.[176] The repackaged medicine was distributed to other assisted-living facilities or the general public and resubmitted to insurance.[177] The pharmacist also paid assisted-living facilities to refer residents.[178] In Baltimore, a pharmacist admitted to purchasing drums of drugs from an unlicensed provider, mislabeling them, and dispensing them to customers.[179] The same pharmacist submitted claims to Medicare for prescription refills that were not dispensed to beneficiaries.[180] Still another pharmacist admitted to paying Medicare and Medicaid beneficiaries for their prescriptions and then submitting reimbursement claims to insurance companies without dispensing the medication.[181] Among his targets were

---

[174] Press Release, U.S. Dep't of Justice, Office of Pub. Affairs, Los Angeles-Area Church Pastor Pleads Guilty to Money Laundering and Conspiring with Doctors, Others to Defraud Medicare of More than $11 Million (Dec. 17, 2012), *available at* http://www.justice.gov/opa/pr/2012/December/12-crm-1506.html.

[175] Scott Bronstein & Drew Griffin, *Dialysis Company Accused of Giant Medicare Fraud*, CNN.COM (Nov. 30, 2012), http://www.cnn.com/2012/11/30/health/medicare-fraud-case/index.html.

[176] Press Release, U.S. Dep't of Justice, Office of Pub. Affairs, Pharmacy Owner Pleads Guilty in Miami for Role in $23 Million Health Care Fraud Scheme (Dec. 6, 2012), *available at* http://www.justice.gov/opa/pr/2012/December/12-crm-1461.html.

[177] *Id.*

[178] *Id.*

[179] Press Release, U.S. Attorney's Office, Dist. of Md., Pharmacy Owner Sentenced to Over 4 Years for Health Care Fraud, Aggravated Identity Theft and Conspiracy to Misbrand Drugs (July 1, 2010), *available at* http://www.justice.gov/usao/md/Public-Affairs/press_releases/press08/PharmacyOwnerSentencedtoover4YearsforHealthCareFraudAggravatedIdentityTheftandConspiracy.html ("Agents recovered drugs from the pharmacies with expiration dates removed and others with altered labels. Agents seized more controlled substances from [the pharmacist]'s home, including Oxycodone, Fentanyl, Adderall and Kadian, all of which were expired.").

[180] *Id.*

[181] Press Release, U.S. Attorney's Office, Dist. of Mass., Dorchester Pharmacist Convicted for Defrauding Medicare and Medicaid (July 20, 2011), *available at* http://www.justice.gov/usao/ma/news/2011/July/McGeePleaPR.html; Press Release, U.S. Attorney's Office, Dist. of Mass., Pharmacist Pleads Guilty to Conspiracy to Defraud Medicaid (Sept. 13, 2010), *available at* http://www.justice.gov/usao/ma/news/2010/

patients with HIV or mental illness, whose medications are particularly expensive.[182]

Patients are not always innocent victims, of course. Beneficiaries often participate in healthcare fraud schemes in exchange for services or kickbacks.[183] Kickbacks range from cash[184] and cigarettes[185] to spa services and lunches.[186] In a massive operation in New York, conspirators paid $500,000 to beneficiaries in a special "kickback room."[187] Some of these schemes are far more Dickensian, providing subsistence benefits, such as housing, to vulnerable beneficiaries and then threatening them with homelessness if they refuse to comply with the fraud.[188] Whether through coercion, persuasion, or deception, individuals engaged in fraud expose Medicare beneficiaries, who are often ill or limited in capacity, to substantial risks.

Medical identity theft is a significant problem as well. CMS reports that, in 2011, a man was convicted of stealing his brother's medical information and using it for surgery covered under his brother's insurance.

September/OnujioguAmadiegwuPleaPR.html.

[182] *See* sources cited *supra* note 181.

[183] The Government Accountability Office reported that about 11% of the successful criminal fraud prosecutions were of beneficiaries. GAO-13-213T, *supra* note 157, at 4.

[184] Mark Schoofs et al., *Medicare-Fraud Crackdown Corrals 114*, WALL ST. J., Feb. 18, 2011, at A3 (reporting that, according to the indictment, the following exchange took place between a provider and a beneficiary: "Beneficiary: 'Each person I refer to you is $200 or $250?' [Provider]: 'I'm going to be honest with you. I will give you $150. Alright $250, $200. [Expletive] I ain't goin fifty 'cause I got to have something now, come on'").

[185] *91 Are Charged with Fraud, Billing Millions to Medicare*, N.Y. TIMES, Oct. 5, 2012, at B5 ("Some patients watched TV instead of receiving services . . . .").

[186] Press Release, U.S. Dep't of Justice, Office of Pub. Affairs, Brooklyn, N.Y., Physician and Clinic President Pleads Guilty to Medicare Fraud Scheme (Dec. 10, 2012), *available at* http://www.justice.gov/opa/pr/2012/December/12-crm-1474.html.

[187] Jerry Markon, *Justice Dept. Charges 94 People with Health-Care Fraud*, WASH. POST, July 17, 2010, at A14; *see also* Press Release, U.S. Dep't of Justice, Office of Pub. Affairs, Brooklyn, N.Y., Clinic Employee Pleads Guilty in Connection with $71 Million Medicare Fraud Scheme (Dec. 3, 2012), *available at* http://www.justice.gov/opa/pr/2012/December/12-crm-1436.html; Press Release, U.S. Dep't of Justice, Office of Pub. Affairs, Owner of Brooklyn Clinic Pleads Guilty in Connection with $71 Million Medicare Fraud Scheme (Dec. 18, 2012), *available at* http://www.fbi.gov/newyork/press-releases/2012/owner-of-brooklyn-clinic-pleads-guilty-in-connection-with-71-million-medicare-fraud-scheme ("In total, 16 individuals have been charged in the Bay Medical scheme, including two doctors, nine clinic owners/operators/employees and five external money launderers."); Press Release, U.S. Dep't of Justice, Office of Pub. Affairs, Two Brooklyn Clinic Employees Plead Guilty in Connection with $71 Million Medicare Fraud Scheme (Nov. 28, 2012), http://www.justice.gov/opa/pr/2012/November/12-crm-1419.html.

[188] Jay Weaver, *Ex-Director of Miami Gardens Mental Health Clinic Imprisoned for 8 Years for Medicare Fraud*, MIAMI HERALD (Dec. 21, 2012), http://www.miamiherald.com/2012/12/21/3152770/ex-director-of-miami-gardens-mental.html#storylink=cpy.

The victim's medical records in turn incorrectly included his brother's HIV-positive status, which put the true beneficiary at risk of receiving medically unnecessary drugs and procedures.[189]

Perpetrators also steal the identities of unsuspecting providers who have already been approved by Medicare in order to file fraudulent claims.[190] In one case, a home-health agency owner stopped paying his licensed personnel and, when they quit, billed hundreds of claims under his former employees' licenses.[191] Organized crime is also involved, creating networks of nonexistent clinics based on stolen provider information, often leading to suspicious claims, such as "[a] pregnant woman who gets an ultrasound exam—from an ear, nose and throat doctor[, a] forensic pathologist whose patients walked into his office, rather than being rolled in with toe tags[, a] dermatologist who conducted heart tests[, or a] psychiatrist who performed M.R.I.'s."[192]

Although some providers' identities are stolen, others lend, rent, or sell their identities to facilitate fraud schemes.[193] Take, for example, a case in New Jersey where a licensed provider was "frequently either not in the office at all, or was in his personal office watching television."[194] He provided "pre-signed, blank prescription forms" to the unlicensed employees who were diagnosing patients.[195] In another case, unlicensed physicians paid a licensed physician "$2,000 a month to review and sign medical records prepared by physician assistants."[196]

---

[189] CTRS. FOR MEDICARE & MEDICAID SERVS., *supra* note 155, at 34.

[190] Michael Wilson & William K. Rashbaum, *Real Patients, Real Doctors, Fake Everything Else*, N.Y. TIMES, Oct. 14, 2010, at A31 ("The scheme sidestepped the cumbersome element of most Medicare schemes, which typically involve pairing up a corrupt doctor with a complicit patient faking an injury.").

[191] Press Release, U.S. Attorney's Office, Dist. of N.J., Toms River, New Jersey Man Admits Posing as a Doctor, Treating Elderly Patients in Medicare Fraud Scheme (July 11, 2011), *available at* http://www.fbi.gov/newark/press-releases/2011/toms-river-new-jersey-man-admits-posing-as-a-doctor-treating-elderly-patients-in-medicare-fraud-scheme.

[192] Wilson & Rashbaum, *supra* note 190, at A31.

[193] Pell, *supra* note 161, at A1 ("Using a sham provider number and a UPS Store address, a scam artist can provide what looks like a real physician's approval for unnecessary or non-existent medical services and equipment for a company that is registered to bill Medicare.").

[194] Press Release, U.S. Attorney's Office, Dist. of N.J., Rahway, New Jersey Man Admits Posing as Licensed Physician in Medicaid and Medicare Fraud Scheme (May 9, 2011), *available at* http://www.fbi.gov/newark/press-releases/2011/rahway-new-jersey-man-admits-posing-as-licensed-physician-in-medicaid-and-medicare-fraud-scheme.

[195] *Id.*

[196] Press Release, U.S. Attorney's Office, N. Dist. of Ill., U.S. Arrests Owners of Home Health Care Business and Suspended Podiatrist on Charges Alleging Medicare and Visa Fraud (July 20, 2011), *available at* http://www.fbi.gov/chicago/press-releases/2011/u.s.-arrests-owners-of-home-health-care-business-and-suspended-podiatrist-on-charges-alleging-medicare-and-visa-fraud; *see also* Press Release, U.S. Attorney's Office, N. Dist. of Ill.,

Healthcare fraud is increasingly accomplished and facilitated by electronic means.[197] Rather than steal patient information on an individual basis, hackers target medical information databases. In May 2012, a group of hackers based in Eastern Europe breached Utah's healthcare database, gaining access to over 780,000 records, including Social Security numbers and medical diagnosis codes.[198] These records are essential for fraudulent billing. According to one report, "an individual healthcare record is worth more on the black market ($50, on average) than a U.S.-based credit card and personal identity with social security number combined."[199] As healthcare fraud moves into the digital arena, traditional methods of detection and prosecution are simply inadequate. A cybercrime requires a cybersolution, which, in the case of healthcare fraud, will almost certainly include Big Data.

C. HOW BIG DATA SERVES GOVERNMENTAL INTERESTS IN PREVENTING, DETECTING, AND PROSECUTING HEALTHCARE FRAUD

The overwhelming majority of data that CMS and its contractors use to detect fraud comes from claims, payment, and referral records.[200] Now that

---

Chicago Area Dermatologist and Psychologist Charged in Nationwide Medicare Fraud Strike Force Takedown (Oct. 4, 2012), *available at* http://www.justice.gov/usao/iln/pr/chicago/2012/pr1004_01.pdf (announcing that two of the defendants were convicted and a third pleaded guilty).

[197] *Compare* Cynthia M. Stamer, *Cybercrime and Identity Theft: Health Information Security Beyond HIPAA*, 1 ABA HEALTH ESOURCE (2005), *available at* https://www.americanbar.org/newsletter/publications/aba_health_esource_home/stamer_right.html (explaining how healthcare identity theft is an increasing problem), *and* Neal Ungerleider, *Medical Cybercrime: The Next Frontier*, FAST COMPANY (Aug. 15, 2012, 3:34 PM), http://www.fastcompany.com/3000470/medical-cybercrime-next-frontier (reporting incidences of medical-record and medical-equipment hacking), *with* Lara Jakes Jordan, *38 Charged in Phishing Scams: Consumer Data Target of Global Ring*, WASH. POST, May 20, 2008, at D3 (describing a general identity-theft operation), Cassell Bryan-Low, *Identity Thieves Organize; Investigators See New Pattern: Criminals Team Up to Sell Stolen Data Over the Internet*, WALL ST. J., Apr. 7, 2005, at B1 (outlining methods of identity theft aimed at financial data), *and* Press Release, U.S. Dep't of Justice, Int'l Cyber-Fraud Ring Responsible for Millions of Dollars in Fraud Dismantled (Dec. 5, 2012), *available at* http://www.justice.gov/opa/pr/2012/December/12-crm-1452.html (publicizing a scheme wherein individuals posted fraudulent vehicle ads on websites).

[198] *Common Questions*, UTAH DEP'T OF HEALTH, DATA BREACH SOLUTION CTR., http://www.health.utah.gov/databreach/common-questions.html (last visited May 21, 2013).

[199] Keith Tyson, *What's the Market Value of a Healthcare Record?*, DELL SECUREWORKS (Dec. 13, 2012), http://www.secureworks.com/media/blog/general/market-value-of-a-healthcare-record/; *see also* Cole Petrochko, *DHC: EHR Data Target for Identity Thieves*, MEDPAGE TODAY (Dec. 7, 2011), http://www.medpagetoday.com/PracticeManagement/InformationTechnology/30074.

[200] CTRS. FOR MEDICARE AND MEDICAID SERVS., *supra* note 155, at 17; *see also* Pasquale,

CMS is partnering with private insurance organizations, it will have access to private claims and other health data.[201] Additionally, the Medicare Integrity Manual lists a dozen types of data that contract agencies should use when investigating suspicious activity, including: (1) the nature of the providers and staff; (2) the structure of the business, overhead costs, and its relationship to other businesses; (3) the amount of business generally and the amount of business from Medicare/Medicaid reimbursements specifically; (4) the types of services rendered; (5) location; (6) history of claims and any previous investigations; and (7) "[o]ther information needed to explain and/or clarify the issue(s) in question."[202]

In part due to the involvement of international organized crime syndicates, the Department of Justice (DOJ), which investigates and prosecutes fraud cases, considers healthcare fraud an indicator of potential terrorism.[203] DOJ describes healthcare providers as "nontraditional information gatherers [that] can provide [interagency data-sharing] fusion centers with both strategic and tactical information,"[204] including "health surveillance networks [and] syndromic surveillance."[205] It recommends that fusion centers, which serve as hubs for local, state, and federal information gathering and sharing,[206] collaborate with healthcare providers to develop analytical tools.[207] Access to fusion-center networks means having the ability to mine and analyze vast public databases at the state, local, and federal level; data-broker dossiers on millions of individuals;

---

supra note 162, at 46 ("The public-private surveillance partnerships pioneered in [HHS and DOJ's] fraud fighting efforts are a model for both the first order problem of collecting and analyzing data and the second order problem of 'watching the watchers' to ensure that data is used properly."); *id.* at 49 (describing the intergration of numerous data sources for the purpose of detecting fraud).

[201] Press Briefing, Attorney General Eric Holder Speaks at the Fraud Prevention Partnership Announcement Event (July 26, 2012), *available at* http://www.stopfraud.gov/iso/opa/stopfraud/ag-speech-120726.html.

[202] MEDICARE PROGRAM INTEGRITY MANUAL 2.4(B) (rev. ed. Nov. 20, 2009), *available at* http://www.cms.gov/Regulations-and-Guidance/Guidance/Manuals/Downloads/pim83c02.pdf.

[203] U.S. DEP'T OF JUSTICE, FUSION CENTER GUIDELINES 13 (2006), *available at* http://www.it.ojp.gov/documents/fusion_center_guidelines_law_enforcement.pdf ("Many experts believe that there is a high probability of identifying terrorists through precursor criminal activity, including illegal drug operations, money laundering, fraud, terrorism, and identity theft.") (internal citation omitted).

[204] *Id.* at 17.

[205] U.S. DEP'T OF JUSTICE, HEALTH SECURITY: PUBLIC HEALTH AND MEDICAL INTEGRATION FOR FUSION CENTERS 6 (2011), *available at* www.it.ojp.gov/docdownloader.aspx?ddid=1450.

[206] *State and Major Urban Area Fusion Centers*, DEP'T OF HOMELAND SEC., http://www.dhs.gov/state-and-major-urban-area-fusion-centers (last visited May 21, 2013).

[207] U.S. DEP'T OF JUSTICE, *supra* note 205, at 8.

private databases held by cooperating entities; video streams from public and private cameras; and far more. In prosecuting fraud cases, DOJ will have access to CMS's data as well as any data aggregated and analyzed by fusion centers. In short, efforts to prevent, detect, and prosecute healthcare fraud are increasingly tied to Big Data.

Already an important tool for regulators and law enforcement, Big Data is likely to become a more powerful and important asset in the years to come.[208] The ACA contains a provision requiring the release of some of Medicare's billing data, which previously had been blocked by a court ruling citing physician privacy.[209] CMS has discussed plans to leverage the detection benefits of Big Data to facilitate a move towards "fraud prevention," rather than the former method of paying claims and later attempting to reclaim funds fraudulently acquired.[210] To this end, CMS has developed multiple task forces and agencies that tap private-sector information technology resources.[211] The most recent initiative is the Fraud Prevention System (FPS), a response to requirements in the Small Business Jobs Act of 2010 "to implement predictive analytics technologies to

---

[208] *See* John Carreyrou & Tom McGinty, *Medicare Records Reveal Troubling Trail of Surgeries*, WALL ST. J., Mar. 29, 2011, at A1; Markon, *supra* note 187, at A14 ("In May 2009, the administration launched a high-level task force, the Health Care Fraud Prevention and Enforcement Action Team, which uses electronic claims data—and the threat of federal prosecution—to seek out illicit billing."); Pasquale, *supra* note 162, at 54 ("[I]t is important to recognize the successes of contractors in utilizing sophisticated data mining to fight fraud. While HHS and DOJ recovered $2.5 billion in 2009, they recovered more than $4 billion in fiscal year 2010. The high-tech Health Care Fraud Prevention & Enforcement Action Team (HEAT) established by the agencies has also enhanced monitoring capacity."); Mark Schoofs & Maurice Tamman, *In Medicare's Data Trove, Clues to Curing Cost Crisis*, WALL ST. J., Oct. 26, 2010, at A1 (describing the preliminary findings revealed by the *Wall Street Journal* and the nonprofit Center for Public Integrity, once they obtained a Medicare provider reimbursement database, and emphasizing the need for greater access to such information).

[209] Ricardo Alonso-Zaldivar, *Feds to Allow Use of Medicare Data to Rate Doctors*, MINN. NPR (Dec. 5, 2011), http://minnesota.publicradio.org/display/web/2011/12/05/feds-allow-medicare-data-to-rate-doctors/ ("Doctors will be individually identifiable through the Medicare files, but personal data on their patients will remain confidential."); *see also* Pasquale, *supra* note 162, at 16. *But see* Robert O'Harrow, Jr, *Health-Care Sector Vulnerable to Hackers, Researchers Say*, WASH. POST (Dec. 28, 2012), http://articles.washingtonpost.com/2012-12-25/news/36015727_1_health-care-medical-devices-patient-care (criticizing the security provisions required by the electronic records program of the American Recovery and Reinvestment Act, which was part of "the Obama administration's first big step toward health-care reform").

[210] Schoofs & Tamman, *Confidentiality Cloaks Medicare Abuse*, *supra* note 162.

[211] For an explanation of the various roles of private contractors in CMS data analysis and fraud detection, see Pasquale, *supra* note 162, at 50–52. *See also* CTRS. FOR MEDICARE AND MEDICAID SERVS., *supra* note 155, at 10 (corporate partners for FPS are Northrop Grumman, Verizon, National Government Services, IBM, and Health Integrity).

identify and prevent the payment of improper claims in the Medicare fee-for-service program."[212]

All of Medicare's daily 4.5 million claims run through FPS's "predictive algorithms and other sophisticated analytics,"[213] which are similar to those used by credit card companies to detect fraudulent purchases.[214] Although FPS cannot automatically stop payments, it "automatically generates and prioritizes leads for review and investigation."[215] FPS addresses the problem of data silos by analyzing claims nationwide[216] and over a period of time,[217] both of which are necessary for identifying fraudulent behavior.[218] FPS also complements the Automated Provider Screening System; the two systems are now slated for integration.[219] CMS has more plans to expand the reach and power of FPS, including social network analysis[220] and adaptive analytics.[221]

According to CMS, in 2011 "FPS also generated leads for 536 new . . . investigations, augmented information for 511 pre-existing investigations, and prompted 617 provider interviews and 1,642 beneficiary interviews to verify legitimate provision of Medicare services and supplies."[222] CMS claims that these efforts resulted in a savings of $115 million.[223] Although modest when compared to the total of $4.1 billion that CMS recovered from fraud schemes through partnerships with private contractors and government agencies in 2011,[224] the program is just getting started, and

---

[212] CTRS. FOR MEDICARE AND MEDICAID SERVS., *supra* note 155, at ii.

[213] *Id.* at iv, 11.

[214] *Id.* at 4, 11.

[215] *Id.* at v, 36.

[216] *Id.* at 8.

[217] *Id.* at 36.

[218] U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-13-104, MEDICARE FRAUD PREVENTION CMS HAS IMPLEMENTED A PREDICTIVE ANALYTICS SYSTEM, BUT NEEDS TO DEFINE MEASURES TO DETERMINE ITS EFFECTIVENESS 6 (2012), *available at* http://www.gao.gov/assets/650/649537.pdf.

[219] CTRS. FOR MEDICARE & MEDICAID SERVS., *supra* note 155, at 25, 37 ("The most effective prevention tool is revoking the billing privileges of providers who are known bad actors.").

[220] *Id.* at vi, 18.

[221] *Id.* at 16.

[222] *Id.* at 23.

[223] *See generally* CTRS. FOR MEDICARE & MEDICAID SERVS., *supra* note 155, at app. A (DEP'T OF HEALTH & HUMAN SERVS., OFFICE OF INSPECTOR GEN., A-17-12-53000, THE DEPARTMENT OF HEALTH AND HUMAN SERVICES HAS IMPLEMENTED PREDICTIVE ANALYTICS TECHNOLOGIES BUT CAN IMPROVE ITS REPORTING ON RELATED SAVINGS AND RETURN ON INVESTMENT (2012)). The methods CMS used to calculate the savings have been criticized.

[224] *About Fraud*, STOP MEDICARE FRAUD, http://www.stopmedicarefraud.gov/aboutfraud/index.html (last visited May 21, 2013).

officials expect to prevent or recover billions of dollars in losses.[225]

Even when FPS was in its infancy, the *Wall Street Journal* drew attention to suspicious providers using simple data analysis of a database "contain[ing] records only through 2008, and includ[ing] the claims of just 5% of randomly selected Medicare beneficiaries."[226] In 2010, the *Journal* described the suspect practices of a physical therapist who later pleaded guilty to healthcare fraud.[227] Among other charges, the doctor submitted a claim for a service that occurred while he was on vacation.[228] The *Journal* used the same comparatively limited data set to identify a surgeon who was practicing in Texas after being temporarily banned from Medicare because he had performed unnecessary and harmful surgeries in New Jersey.[229] The *Journal* found that the readmitted doctor's death rate was seven times higher than the national average.[230] Another surgeon appeared to perform an unusually high number of multiple spinal operations per patient.[231]

Investigating these types of activities requires access to Big Data. With Big Data, governmental systems can identify providers who bill more over a specified time period than other providers in the region. Claims analysis can detect providers who authorize particularly expensive equipment. Analysis of individuals' claims over time can reveal discrepancies or impossibilities, such as multiple hysterectomies, which indicate possible identity theft or kickbacks. Looking at groups of individual claims could also reveal possible kickbacks if, for instance, a sizeable population in a community suddenly switches to a less convenient pharmacy. As FPS incorporates social network models, the system will gain further leverage on its data, allowing it to compare individuals against known criminal associations, including those that work primarily in the

---

[225] *HEAT Task Force*, STOP MEDICARE FRAUD, http://www.stopmedicarefraud.gov/aboutfraud/heattaskforce/index.html (last visited May 21, 2013).

[226] Schoofs & Tamman, *supra* note 162; *see also* Carreyrou & McGinty, *supra* note 208 ("For the past year, the Journal has been mining Medicare's claims databases to expose how some doctors potentially defraud the taxpayer-funded health program for the elderly and disabled and game its reimbursement system."). In December 2011, HHS decided to release more information about doctors who participate in Medicare in response to provisions in the Affordable Care Act. *See* John Carreyrou, *Access to Widen on Medicare Data*, WALL ST. J., Dec. 8, 2011, at A6.

[227] Mark Schoofs, *Medicare Fraud Nets Guilty Plea*, WALL ST. J., May 14, 2011, at A3.

[228] *Id.*

[229] Carreyrou & McGinty, *supra* note 208, at A16.

[230] *Id.* ("In 2008 and 2009, nine of 49 Medicare patients on whom he performed an elective surgery died, three of them within days of the operation, according to the Medicare data. That equates to 18.4 deaths per 100 of the procedures, compared with a national average of 2.4 per 100 for the procedure.").

[231] *Id.*

virtual world of black-market healthcare data. The more data the system can use to build comparative models, the more accurately the models will reflect standard practice.[232] As evidence of this potential, CMS recently credited "sophisticated data analysis" for the indictment of a home-healthcare physician in "the biggest health-care fraud case brought against a single doctor."[233] The doctor certified over 5,000 patients a year for home-healthcare by having his employees complete certification forms using his forged signature.[234]

Although many healthcare fraud cases originate through direct reporting, including *qui tam* actions, complicated schemes like those involving organized crime are more vulnerable to data analysis, which can review and compare large volumes of claims over time. To achieve its stated goal of stopping fraudulent payments before they reach the provider, CMS will need robust analytical tools that can probe massive quantities of disparate data to flag automatically suspect claims across a wide range of covered services and also evolve to identify new fraudulent behavior as it develops. That capacity is likely to be greatly enhanced in coming years as CMS programs gain access to the vast quantities of consumer and other data currently brokered through third-party aggregators. At each turn, the government and its agents will face potential Fourth Amendment barriers erected by the mosaic theory of Fourth Amendment privacy.

D. STRIKING A REASONABLE BALANCE BETWEEN PRIVACY INTERESTS AND LEGITIMATE GOVERNMENTAL INTERESTS IN PREVENTING, DETECTING, AND PROSECUTING HEALTHCARE FRAUD

According to the mosaic theory, gathering the large quantities of information engaged by Big Data raises significant Fourth Amendment privacy issues—all the more so when that data is processed through sophisticated analytical software. Although troubling from a privacy point of view, the foregoing shows that the government's interest in Big Data is

---

[232] *But see* Robert Radick, *Claims Data and Health Care Fraud: The Controversy Continues*, FORBES (Sept. 25, 2012, 11:50 AM), http://www.forbes.com/sites/insider/2012/09/25/claims-data-and-health-care-fraud-the-controversy-continues/ (criticizing reliance on claims data that CMS officials have admitted can be inaccurate).

[233] Sari Horwitz, *Tex. Doctor Charged in $375 Million Health-Care Scam, Largest of Its Kind*, WASH. POST, Feb. 29, 2012, at A1 ("[The] alleged scheme resulted in more than $350 million being fraudulently billed to Medicare and more than $24 million to Medicaid.").

[234] *Id.* The doctor's home also contained incriminating evidence, including "the books 'Hide Your Assets and Disappear: A Step-by-Step Guide to Vanishing Without a Trace,' and 'The Offshore Money Manual,' suggesting 23 worldwide locations favorable to offshore banking." *Id.*

not nefarious or idle. Rather, it is rationally tied to legitimate regulatory and law enforcement interests in preventing, detecting, and prosecuting various forms of Medicare and healthcare fraud.

The mosaic theory would certainly impact these legitimate governmental interests. It would not, however, bar access to Big Data. Rather, where a law enforcement method, practice, or technology encroaches upon reasonable expectations of privacy, the mosaic theory will require that access and use be limited and constrained to effect a "reasonable" balance between law enforcement interests and citizens' privacy interests.[235] In the context of physical searches of the home, the warrant requirement does this work.[236] But, for Big Data, the warrant requirement would fail to strike a reasonable balance because it would render the technology largely useless from the government's point of view. The whole point of Big Data is, after all, to gather large quantities of data and to submit it to analysis without having any specific prior suspicions of wrongdoing by particular people. On the other hand, granting law enforcement unfettered access to Big Data and its products would effectively leave unrecognized and unprotected important quantitative privacy interests. The challenge going forward, then, will be for government officials and their private-sector contractors to work with interest groups, academics, legislators, and ultimately the courts to tailor Big Data programs in ways that effect a reasonable balance of these competing interests. Although it is beyond the scope of the present Article to do so, we offer a sketch below of what some of the broad framework might look like.[237]

---

[235] *See* Gray & Citron, *supra* note 7, at 28.

[236] Johnson v. United States, 333 U.S. 10, 13–14 (1948) ("The point of the Fourth Amendment, which often is not grasped by zealous officers, is not that it denies law enforcement the support of the usual inferences which reasonable men draw from evidence. Its protection consists in requiring that those inferences be drawn by a neutral and detached magistrate instead of being judged by the officer engaged in the often competitive enterprise of ferreting out crime. Any assumption that evidence sufficient to support a magistrate's disinterested determination to issue a search warrant will justify the officers in making a search without a warrant would reduce the Amendment to a nullity and leave the people's homes secure only in the discretion of police officers. Crime, even in the privacy of one's own quarters, is, of course, of grave concern to society, and the law allows such crime to be reached on proper showing. 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.").

[237] *See infra* Part IV.D; *see also* Gray & Citron, *supra* note 7, at 35–40.

IV. HOW DIGITAL SURVEILLANCE SERVES GOVERNMENTAL INTERESTS IN PREVENTING, DETECTING, AND PROSECUTING CYBERHARASSMENT

As Justice Alito notes in his *Jones* concurrence, we no longer live in a "pre-computer age."[238] Quite to the contrary, whether in the form of personal computers, tablets, smartphones, cellular phones, video games, the Internet, e-mail, or GPS-enabled directional devices, technology is a ubiquitous feature of our daily lives. Access to these technologies has the capacity to expand our lives and life projects dramatically by enhancing efficiency and giving us ready and immediate access to information and people. These technologies are, in short, liberty enhancing. The expansion of personal and associational liberties offered by modern technologies is not entirely free, however. To the contrary, as Justice Alito points out, much of the increased "convenience" and "security" promised by modern technology comes "at the expense of privacy."[239] Building on contributions to the privacy law project since Samuel Warren and Louis Brandeis's seminal 1890 article,[240] Justice Alito and others have elaborated many of these privacy costs. Their worries are particularly weighty when the government is the observer.[241]

Everything we do is subject to digital surveillance. When we visit websites, we leave traceable footprints that include information about our Internet service providers (ISPs) and the Internet protocol (IP) addresses associated with our computers.[242] Most websites deposit cookies on our

---

[238] United States v. Jones, 132 S. Ct. 945, 963 (2012) (Alito, J., concurring in the judgment).

[239] *Id.* at 962. Some have argued that this apparent conflict between law enforcement interests and citizen privacy interests is a "myth." *See, e.g.*, Weinstein, *supra* note 118, at 38–39. Although important, these arguments actually address another point. Specifically, they point out that law enforcement interests in digital surveillance, say, are derived directly from significant citizen privacy and security interests that are best preserved by success in detecting and prosecuting crimes like identity theft and cyberharassment. This is no doubt true, but it does not render the conflict moot. Rather, recognizing the citizen interests that stand behind law enforcement interests adds depth and clarity to the crime-control side of the Fourth Amendment balancing test. Whether and how far to service those interests still requires taking account of how much privacy it is reasonable to sacrifice to the "competitive enterprise of ferreting out crime." *Johnson*, 333 U.S. at 14 .

[240] Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

[241] *Jones*, 132 S. Ct. at 957 (Sotomayor, J., concurring); *id.* at 964 (Alito, J., concurring in the judgment); Gray & Citron, *supra* note 7, at 23–27.

[242] Although IP addresses are not fixed to our computers, they change less often than was once the case, and many ISPs have reverted to using permanent or semipermanent IP addresses for users. As a consequence, tracing Internet activity using IP addresses provides more information now than it did even a few years ago, when limited bandwidth often required ISPs to reassign a limited number of IP addresses to users as they logged on and off the Internet.

computers that provide information about our activities to site operators, other websites, and advertisement brokers. Documents sent via networks, including e-mail and texts, contain a wealth of information, including metadata with time stamps, location information, and other details about our activities. Programs and applications we use on our computers and portable devices record and share locational data, pictures, and other information about us.

These vast reservoirs of our location data, e-mails, cookies, and the like are prime targets for cyberharassers who want to control, intimidate, and terrify victims. Harassers hack into victims' computers and portable devices to track their whereabouts. Once inside victims' computers, they forward victims' sensitive e-mails and intimate pictures to their employers and friends. But, as we shall see, the digital surveillance technologies that gather information from these sources can also assist the government in its pursuit and prosecution of cyberharassers. As in Part III, we begin by briefly describing how digital surveillance implicates a mosaic theory of Fourth Amendment privacy.

A. DIGITAL SURVEILLANCE AND THE MOSAIC THEORY

Most of us have at best a vague sense of what and how much digital data we generate and share, much less the extent of digital surveillance we are subjected to by those who gather, aggregate, and analyze that data. Nevertheless, social networking sites, merchants, and data brokers record and analyze our digital footprints. Some do so for immediate commercial gain by, for example, targeting advertisements. Some package the information into "digital dossiers," which they sell to government and private clients.[243] Law enforcement and other government officials routinely contract with these data brokers or directly request or subpoena information about our online activities from ISPs, e-mail providers, and search engines.[244]

Government agencies are also directly involved in digital surveillance. On an investigative level, federal agents who nobly pursue child pornographers use a toolkit of devices—including "Wifinders" and proprietary peer-to-peer software, along with strategies like "wardriving"—to identify computers that are engaged in distributing child pornography

---

[243] DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE 2 (2004).

[244] Scott Shane and John F. Burns, *Twitter Records in Wikileaks Case Are Subpoenaed*, N.Y. TIMES, Jan. 8, 2011, at A1. For example, Google reports that it received over 8,000 requests for information from agencies in the United States between July and December 2012. *Transparency Report: United States*, GOOGLE, https://www.google.com/transparency report/userdatarequests/US/ (last visited May 21, 2013).

and to find images of child pornography on suspects' hard drives.[245] The *Wall Street Journal* recently reported that the National Counterterrorism Center has been "grant[ed] authority for unprecedented government surveillance of U.S. citizens" using aggregated data, regardless of whether targets are suspected of criminal activity.[246] As a result of this new authorization, the Center will have access to most government databases, potentially including financial information processed through federally guaranteed mortgage programs and health records for anyone treated at a federal facility or covered by federal insurance programs, such as Medicare and Medicaid.[247] Perhaps most ominously, a network of fusion centers, which are operated jointly by law enforcement, intelligence agencies, and private contractors, and sit at strategic Internet and communications chokepoints, appear to have realized the vision of the Department of Defense's much-maligned Total Information Awareness program.[248]

This web of digital surveillance is so broad and subtle, in fact, that it was able to snare former Central Intelligence Agency Director David Petreaus.[249] During the course of an investigation into allegedly harassing e-mails sent to a Tampa-area event planner, FBI agents used metadata, ISP information, IP addresses, and, eventually, a warranted electronic search of an e-mail account, to determine that the suspect mails were sent by Petraeus's biographer, Paula Broadwell.[250] As a by-product, investigators also discovered evidence of an extramarital affair between Petraeus and

---

[245] United States v. Budziak, 697 F.3d 1105, 1107–08 (9th Cir. 2012); United States v. Chiaradio, 684 F.3d 265, 271–72 (1st Cir. 2012); United States v Gorski, 71 M.J. 729, 731–32 (Army Ct. Crim. App. 2012); United States v. Ahrndt, 3:08-CR-00468-KI, 2013 WL 179326, at *1–3 (D. Or. Jan. 17, 2013); United States v. Broadhurst, 3:11-CR-00121-MO-1, 2012 WL 5985615, at *1–2 (D. Or. Nov. 28, 2012); United States v. Stanley, Crim. No. 11-272, 2012 WL 5512987, at *2 (W.D. Pa. Nov. 14, 2012); Press Release, Dep't of Justice, Lincolnton Man Sentenced to 87 Months in Prison on Child Pornography Charges (Aug. 9, 2012), http://www.justice.gov/usao/ncw/pressreleases/Charlotte-2012-08-09-byrd.html. As we point out below and elsewhere, we see both the investigative self-constraints and technological precommitments under which these technologies operate as examples of precisely where and how agencies, legislatures, and courts should strike the reasonable balance required by the Fourth Amendment after *Jones*. *See* Gray & Citron, *supra* note 7.

[246] Julia Angwin, *U.S. Terror Agency to Tap Citizen Files*, WALL ST. J., Dec. 13, 2012, at A1.

[247] *Id.*

[248] Danielle Keats Citron & Frank Pasquale, *Network Accountability for the Domestic Intelligence Apparatus*, 62 HASTINGS L.J. 1441, 1443 (2011).

[249] Evan Perez et al., *FBI Scrutinized on Petraeus—Complaints by Female Social Planner Led to Email Trail that Undid CIA Chief*, WALL. ST. J., Nov. 12, 2012, at A1; Scott Shane & Charlie Savage, *Officials Say F.B.I. Knew of Petraeus Affair in the Summer*, N.Y. TIMES (Nov. 11, 2012), http://www.nytimes.com/2012/11/12/us/us-officials-say-petraeuss-affair-known-in-summer.html?pagewanted=all.

[250] Perez et al., *supra* note 249; Shane & Savage, *supra* note 249.

Broadwell, the revelation of which led Petraeus to resign from his position at the CIA. Marc Rotenberg, executive director of the Electronic Privacy Information Center, noted that this kind of investigation creep is "a particular problem with cyber investigations [in that] they rapidly become open-ended because there's such a huge quantity of information available and it's so easily searchable."[251] Commenting on the potential privacy threats of digital surveillance, Rotenberg pointed out that "[i]f the C.I.A. director can get caught, it's pretty much open season on everyone else."[252]

As the *Wall Street Journal* notes, digital surveillance programs like fusion centers and the initial stages of the probe that led to the discovery of Petraeus's affair are outside the scope of Fourth Amendment review because they involve information that is either exposed to public observation or voluntarily shared with third parties.[253] They are, however, precisely the sorts of investigative technologies, methods, and techniques that a mosaic theory of Fourth Amendment privacy would encompass. They are broad, indiscriminate, capable of almost infinite expansion, and therefore not subject to the practical constraints that limit more traditional surveillance techniques.[254] They are also surreptitious and therefore "susceptible to abuse."[255] In short, granting the "Government . . . unfettered discretion" to engage in digital surveillance threatens to "alter the relationship between citizen and government in a way that is inimical to democratic society."[256]

Given the invasive potential of digital surveillance, it is easy to see, from a citizen privacy point of view, why digital surveillance and other cyberinvestigative techniques should be subject to Fourth Amendment regulation. As explained in Part II, however, "regulation" does not mean prohibition. Rather, limiting law enforcement's discretion to engage in digital surveillance will require balancing these Fourth Amendment privacy concerns against legitimate governmental interests in detecting and

---

[251] Scott Shane, *Petraeus Case: Issue of Privacy Is in Play Too*, N.Y. TIMES, Nov. 14, 2012, at A1.

[252] *Id.*

[253] Angwin, *supra* note 246 (stating that the Fourth Amendment "doesn't cover records the government creates in the normal course of business with citizens").

[254] United States v. Jones, 132 S. Ct. 945, 963 (2012) (Alito, J., concurring in the judgment); *see also* Gray & Citron, *supra* note 7, at 28–41 (arguing that technology capable of facilitating broad and indiscriminate surveillance should be subject to Fourth Amendment regulation).

[255] *Jones*, 132 S. Ct. at 956 (Sotomayor, J., concurring); *see also* Susan Freiwald, *The Four Factor Test*, USVJONES.COM, http://usvjones.com/2012/06/04/the-four-factor-test/#more-205 (last visited May 21, 2013) (arguing that the capacity to conduct surreptitious surveillance is a significant factor in evaluating Fourth Amendment regulation).

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

prosecuting crime. In the next section we explore one such area of law enforcement interest: cyberharassment.

B. THE VALUE OF DIGITAL SURVEILLANCE IN COMBATING CYBERHARASSMENT

Cyberharassment is a widespread and growing challenge for law enforcement in the United States. These online attacks feature threats of violence, privacy invasions, reputation-harming falsehoods, impersonation, computer hacking, and extortion. They often appear in e-mails, instant messages, blog entries, message boards, or sites devoted to tormenting individuals. As the executive director of the National Center for Victims of Crime explained in her congressional testimony supporting the 2006 cyberstalking amendment to the Violence Against Women Act:

> [S]talkers are using very sophisticated technology . . . —installing spyware on your computer so that they can track all of your interactions on the Internet, your purchases, your e-mails and so forth, and then using that against you, forwarding e-mails to people at your job, broadcasting your whereabouts, your purchases, your reading habits and so on, or installing GPS in your car so that you will show up at the grocery store, at your local church, wherever and there is the stalker and you can't imagine how the stalker knew that you were going to be there. . . . I am happy that this legislation amends the statute so that prosecutors have more effective tools, I think, to address technology through VAWA 2005.[257]

Although some attackers confine their harassment to networked technologies, others use all available tools to harass victims, including real-space contact. Offline harassment or stalking often includes abusive phone calls, vandalism, threatening mail, and physical assault.[258]

According to the Bureau of Justice Statistics, 850,000 adults experienced stalking with an online component in 2006, including threats in e-mails, text messages, chat rooms, and blogs.[259] Young people are even more likely to experience some form of cyberharassment. The National Center for Education Statistics reports that, during the 2008–2009 school year, 1.5 million young people in the United States were victims of some form of cyberharassment.[260] Already a significant problem,

---

[257] *Reauthorization of the Violence Against Women Act: Hearing Before the S. Comm. on the Judiciary*, 109th Cong. 18, 27–28 (2005) (statement of Mary Lou Leary, Executive Director, National Center for Victims of Crime).

[258] WORKING TO HALT ONLINE ABUSE, *supra* note 12.

[259] CITRON, *supra* note 8 (citing KATRINA BAUM ET AL., BUREAU OF JUSTICE STATISTICS, U.S. DEP'T OF JUSTICE, STALKING VICTIMIZATION IN THE UNITED STATES 5 (2009)).

[260] NAT'L CTR. FOR EDUC. STATISTICS, U.S. DEP'T OF EDUC., STUDENT REPORTS OF BULLLYING AND CYBER-BULLYING: RESULTS FROM THE 2009 SCHOOL CRIME SUPPLEMENT TO THE NATIONAL CRIME VICTIMIZATION SURVEY 1 (2009), *available at* http://nces.ed.gov/pubsearch/pubsinfo.asp?pubid=2011336.

cyberharassment is on the rise. College students now report more sexually harassing speech in online interactions than in face-to-face ones. As the National Institute of Justice explains, the "ubiquity of the Internet and the ease with which it allows others unusual access to personal information" make individuals more accessible and vulnerable to online abuse.[261] Harassing someone online is far cheaper and less personally risky than confronting them in real space.[262]

Cyberharassment and the identity of its victims follow the well-worn pathways of bias crimes. The most recent Bureau of Justice Statistics findings report that 74% of online stalking victims are female.[263] Perpetrators are far more likely to be men.[264] Unsurprisingly, the content of these attacks are often sexually explicit and demeaning, drawing predominantly on gender stereotypes. As one blogger observed, "[t]he fact is, to be a woman online is to eventually be threatened with rape and death. On a long enough timeline, the chances of this not occurring drop to

---

[261] Cyberharassment is so easy, in fact, that it has spawned a new breed of social creature, the troll, who engages in provocative, and sometimes obscene, vitriolic, abusive, or hateful speech, in order to generate strong emotional responses. Whitney Phillips provides a useful history of Internet trolls in a recent essay published in *The Atlantic* online. Whitney Phillips, *What an Academic Who Wrote Her Dissertation on Trolls Thinks of Violentacrez*, THEATLANTIC.COM (Oct. 15, 2012, 12:32 PM), http://www.theatlantic.com/technology/archive/2012/10/what-an-academic-who-wrote-her-dissertation-on-trolls-thinks-of-violentacrez/263631/. As Phillips points out, the phenomenon of Internet trolling is complicated from a postcritical, sociocultural point of view. After all, many trolls are less than sincere, either because they are thoughtfully ironic or because they get a base thrill out of causing offense. Most trolls also keep it impersonal and do not engage in personal or exploitative attacks. They are the satirists of our age, and play an important role in online discourse. For some trolls, however, manners, sophistication, empathy, and humility do not advise such restraint. As Phillips points out, whether the conduct of these trolls masks or reveals their true opinions is pretty nearly irrelevant. After all, "whether or not the troll 'really' hates women, for example, doesn't matter if the targeted women feel hated." *Id.* We discuss the recent unmasking of one troll, "Violentacrez," below.

[262] *Stalking*, NAT'L INST. OF JUSTICE, http://www.nij.gov/topics/crime/stalking/welcome.htm (last visited May 21, 2013).

[263] CITRON, *supra* note 8, at 5 (citing BAUM ET AL., *supra* note 259, at 5). Similarly, statistics from the National Center for Victims of Crime find that 70% of stalking cases involve female victims. *Id.* The U.S. National Violence Against Women Survey reports that 60% of cyberstalking victims are women. *Id.* (citing Molly M. Ginty, *Cyberstalking Turns Web Technologies into Weapons*, OTTAWA CITIZEN, Apr. 7, 2012, at J1). A University of Maryland study of online attacks showed that users with female names received on average 100 malicious private messages, which the study defined as "sexually explicit or threatening language," for every four received by male users. CITRON, *supra* note 8, at 5 (citing ROBERT MEYER AND MICHEL CUKIER, ASSESSING THE ATTACK THREAT DUE TO IRC CHANNELS 467–72 (2006)).

[264] Women were more likely to be targeted by men (67%) than women (24%). CITRON, *supra* note 8, at 5 (citing BAUM ET AL., *supra* note 259, at 4).

zero."[265]

Cyberharassment also follows racial lines. A study conducted in 2009 asked 992 undergraduate students about their experience with cyberharassment. According to this study, nonwhite females faced cyberharassment more than any other group, with 53% reporting having been harassed online. Next were white females, with 45% reporting having been targeted online, with nonwhite males right behind them at 40%. The group least likely to have been harassed was white males, at 31%.[266] Across race, being lesbian, transgender, or bisexual also raised the risk of being harassed.[267]

Another disturbing feature of cyberharassment is that it tends to be perpetrated by groups rather than individuals. Those who engage in abusive online conduct often move in packs.[268] Cyberharassers frequently engage proxies to help torment their victims.[269] These group attacks bear all of the hallmarks of violent mob behavior. So much so, in fact, that one of us has dubbed them "cyber mobs."[270] As with sole practitioners, online mob harassment is more likely to be perpetrated by members of dominant demographics, and to draw on popular stigmas for the purpose of shaming and degrading their targets.[271]

Of course, cold statistics and general description tell at best part of the story of legitimate government and law enforcement interests in preventing, detecting, and prosecuting cyberharassment. Recent efforts to highlight the privacy interests that compel recognition of the mosaic theory of Fourth Amendment privacy make liberal use of individual stories, in part to pluck

---

[265] Yuki Onna, *Let Me Tell You About the Birds and the Bees: Gender and the Fallout Over Christopher Priest*, RULES FOR ANCHORITES: LETTERS FROM PROXIMA THULE (Apr. 6, 2012), http://yuki-onna.livejournal.com/675153.html.

[266] Bradford W. Reyns, Being Pursued Online: Extent and Nature of Cyberstalking Victimization from a Lifestyle/Routine Activities Perspective 96–97 (May 7, 2010) (unpublished Ph.D. dissertation, University of Cinicinnati), *available at* http://etd.ohiolink.edu/send-pdf.cgi/Reyns%20Bradford%20W.pdf?ucin1273840781.

[267] Lisa Stone of *BlogHer* has observed that the more famous, the more lesbian, and the more non-white the female blogger, the more vicious the cyberharassment. Lisa Stone, *Hating Hate Speech: Safety for Kathy Sierra and All Women Online*, BLOGHER (Mar. 27, 2007, 1:47 AM), http://www.blogher.com/hating-hate-speech-safety-kathy-sierra-and-all-women-online.

[268] CITRON, *supra* note 8, at 9.

[269] PAUL BOCIJ, CYBERSTALKING: HARASSMENT IN THE INTERNET AGE AND HOW TO PROTECT YOUR FAMILY 67 (2004).

[270] Citron, *Cyber Civil Rights*, *supra* note 13, at 104, 113.

[271] Martha C. Nussbaum, *Objectification and Internet Misogyny*, *in* THE OFFENSIVE INTERNET: SPEECH, PRIVACY, AND REPUTATION 68, 73 (Saul Levmore & Martha Nussbaum eds., 2010).

empathetic strings in the audience.[272] In weighing the competing interests at stake in regulating access to and use of digital surveillance technologies, it is therefore fair to consider the impact of crimes like cyberharassment in individual cases.

Take the publicly reported case of *D.C. v. R.R.*[273] D.C. was a high school student who was actively pursuing a career in the entertainment industry as a singer and actor.[274] He used a pseudonym in his professional career,[275] under which he maintained a fan site that, among other features, allowed visitors to post comments to a "guestbook." Several students at D.C.'s school, who were later identified in a civil suit, engaged in a pattern of targeted harassment of D.C. by posting comments to his website. Some were simply offensive—one student told D.C. that he was "the biggest fag in the [high school] class."[276] Others, however, went much further, threatening physical and sexual violence in graphic detail. One person posted on D.C.'s website, "I want to rip out your fucking heart and feed it to you. . . . If I ever see you I'm . . . going to pound your head in with an ice pick. Fuck you, you dick-riding penis lover. I hope you burn in hell."[277] Another post told D.C. that he was "now officially wanted dead or alive," and a third promised to "unleash my manseed in those golden brown eyes."[278]

According to a California appellate court, the contents of these posts suggested that "[t]he students . . . sought to destroy D.C.'s life, threatened to murder him, and wanted to drive him out of [his high school] and the community in which he lived."[279] In that goal they were successful. On

---

[272] *See* Tamara Rice Lave, Privacy, Poverty, and People Like Us: Rethinking the Fourth Amendment after *US v Jones* (unpublished manuscript) (on file with authors) (arguing that Fourth Amendment privacy interests only gain traction once a critical mass of citizens on and off the courts feel that their personal expectations of privacy are threatened).

[273] D.C. v. R.R., 106 Cal. Reptr. 3d 399 (Ct. App. 2010).

[274] *Id.* at 405.

[275] *Id.* at 409.

[276] *Id.* at 412.

[277] *Id.* at 422.

[278] *Id.* at 406.

[279] *Id.* The students who posted to D.C.'s website disputed this conclusion. Despite the vivid, violent, and homophobic content of his post, one student claimed:

> My motivations in sending this email had nothing to do with any perception of [D.C.'s] sexual orientation, and certainly did not reflect an intention to do him physical harm. As set forth above, I had no personal knowledge or belief about [D.C.'s] sexual orientation. No one ever told me he was gay, and I had no thoughts on the subject matter. My message is fanciful, hyperbolic, jocular, and taunting and was motivated by [D.C.'s] pompous, self aggrandizing, and narcissistic website—not his sexual orientation. My only other motivation, a bit more pathological, was to win the one-upmanship contest that was tacitly taking place between the message posters.

Id. at 410 (alterations in original). The California court noted, however, that in cases of

advice of law enforcement, who consulted the Federal Bureau of Investigation, D.C. withdrew from his school and moved with his family to the other end of the state.[280] Despite these efforts, the student newspaper at his former school reported his new location and the name of his new institution.[281] As a consequence of this harassment, D.C. developed a persistent anxiety disorder.[282]

Cyberharassment has also spawned a new brand of extortion labeled "sextortion."[283] This is a form of blackmail in which the extortionist threatens to publicize images or information that his target might find embarrassing unless the victim provides sexually explicit pictures and videos or agrees to participate in live sex shows via Skype or other direct video communications.[284] One infamous perpetrator of sextortion schemes invaded his targets' computers using malicious software that allowed him to mine his victims' hard drives for compromising images or to capture images using their own computer cameras.[285] He then used those images and access to his targets' computers and e-mail accounts to terrorize them until they agreed to produce sexually explicit pictures or videos for him. Young people are particularly vulnerable.[286] Teenagers who are extorted into engaging in explicit sex acts under threat and at such a formative stage of their development are also more likely to suffer scarring emotional and psychological harm.[287] As United States Attorney Joseph Hogsett put the

---

tortious threats, "[t]he speaker need not actually intend to carry out the threat." *Id.* at 414 (quoting Virginia v. Black, 538 U.S. 343, 360 (2003)).

[280] *Id.* at 406.

[281] *Id.*

[282] *Id.* at 408.

[283] *See* Charles Wilson, *Feds: Online 'Sextortion' of Teens on the Rise*, NBC NEWS (Aug. 15, 2010, 2:39 PM), http://www.msnbc.msn.com/id/38714259/ns/technology_and_science-security/t/feds-online-sextortion-teens-rise#.UOpEpm_AeSo (describing the crime and recounting the facts of several cases).

[284] Press Release, Dep't of Justice, Maine Resident Charged and Arrested for Allegedly Engaging in Cyber "Sextortion" of New Hampshire Victim (July 18, 2012), *available at* http://www.justice.gov/opa/pr/2012/July/12-crm-886.html.

[285] Nate Anderson, *How an Omniscient Internet "Sextortionist" Ruined the Lives of Teen Girls*, ARS TECHNICA (Sept. 7, 2011, 1:02 PM), http://arstechnica.com/tech-policy/2011/09/how-an-omniscient-internet-sextortionist-ruined-lives/.

[286] Wilson, supra note 283; Press Release, Fed. Bureau of Investigation, Indiana Man Charged with Interstate Sextortion of Children (Apr. 9, 2012), *available at* http://www.fbi.gov/indianapolis/press-releases/2012/indiana-man-charged-with-interstate-sextortion-of-children (reporting the Federal Bureau of Investigation arrest of an Indiana man for using this scheme to extort two fourteen-year-old boys into recording sexually explicit videos).

[287] U.S. DEP'T OF JUSTICE, THE NATIONAL STRATEGY FOR CHILD EXPLOITATION PREVENTION AND INTERDICTION: REPORT TO CONGRESS 1 (2010), *available at* http://www.justice.gov/psc/docs/natstrategyreport.pdf.

point when commenting on a successful prosecution, "This defendant may not remember his alleged victims, but the true tragedy is that not one of them will ever forget."[288]

Cyberharassers engage in telephone harassment as well. For example, in September 2010, Daniel Leonard pleaded guilty to a pattern of harassment that involved over 4,000 threatening and sexually explicit phone calls made to over 1,200 phone numbers using an Internet "spoofing" service that masked his phone number from the call recipients.[289] Others go further still by using the Internet to incite others to rape and stalk victims.

Federal prosecutors recently brought a cyberstalking indictment against a man who impersonated his ex-girlfriend online over a four-year period, inciting others to stalk her in person. The man posted online advertisements with the victim's contact information and her alleged desire for sex with strangers. On porn sites, he uploaded videos of her having sex (which he filmed while they were dating) alongside her contact information.[290] Because strange men began appearing at her home demanding sex, the woman changed her name and moved to another state. Her ex-boyfriend discovered her new personal information and again posted her name, address, and an invitation to have sex on pornography sites next to her picture. The cycle repeated itself, with strange men coming to her house at night demanding sex. Although this victim was never physically assaulted, others are not so lucky.

In December 2009, Ty McDowell broke into the home of a woman in Casper, Wyoming, tied her up, and raped her. During the course of the

---

[288] Press Release, Fed. Bureau of Investigation, *supra* note 286.

[289] Press Release, Dep't of Justice, Olympia Resident Pleads Guilty to Cyber-Stalking, Threatening and Obscene Phone Calls Using Internet 'Spoofing' Service (Sept. 14, 2010), *available at* http://www.justice.gov/criminal/cybercrime/press-releases/2010/leonardPlea.pdf.

[290] United States v. Sayer, Crim. Nos. 2:11-CR-113-DBH, 2:11-CR-47-DBH, 2012 WL 1714746 (D. Me. May 15, 2012); Susan Brenner, *Wi-Fi*, *Curtilage and* Kyllo, CYB3RCRIM3 (June 27, 2012, 11:15 AM), http://cyb3rcrim3.blogspot.com/2012/06/wi-fi-curtilage-and-kyllo.html; Judy Harrison, *Biddeford Man Sentenced to Five Years in Federal Prison for Cyberstalking*, BANGOR DAILY NEWS (Dec. 4, 2012, 3:59 PM), http://bangordailynews.com/2012/12/04/news/portland/biddeford-man-sentenced-to-five-years-in-prison-for-cyberstalking/. Shawn Memarian pleaded guilty to cyberstalking under 18 U.S.C. § 2261A(2)(B)(i), admitting that he sent threatening e-mails to the victim and created fake personal advertisements in which he impersonated the victim, provided her home address, and claimed her interest in sex after which over thirty men showed up at her house seeking sex. Report and Recommendation to Accept Defendant's Guilty Plea, United States v. Memarian, No. 08-00128-01-CR-W-NKL (W.D. Mo. Jan. 9, 2009); News Release, Office of the U.S. Attorney for the W. Dist. of Mo., KC Man Sentenced for Cyberstalking (June 17, 2009), *available at* http://www.justice.gov/usao/mow/news2009/memarian.sen.htm.

attack, he told her: "You want an aggressive man, bitch, I'll show you aggressive."[291] Although McDowell did not know his victim, his crime was not random. Rather, he had responded to an online advertisement posted on Craigslist that purported to be from a woman seeking to fulfill her own rape fantasies. After a lengthy correspondence with the ad's poster, McDowell believed that he was fulfilling his victim's desires.[292] He was not. As a subsequent investigation would reveal, McDowell was in communication with Jebediah Stipe, who posted the ad and arranged the attack on his ex-girlfriend.[293] Stipe and McDowell were sentenced to sixty-year prison terms after pleading guilty to charges of aggravated kidnapping, rape, and burglary.[294]

Cyberharassment can also be more general. Sites that encourage sexualized online abuse are all too common. The website *IsAnyoneUp.com* provides a notorious example. For a time, it was one of the most popular forums on the Internet for "revenge porn," which entails spurned former lovers posting sexualized pictures of their ex-wives and ex-girlfriends on a public forum so that others can leer at and demean them.[295] Although *IsAnyoneUp.com* eventually shut down amidst protests and outcry, its operator, Hunter Moore, started a similar site under a different name, *HunterMoore.TV*, which may eventually include not only pictures of women, but also an overlaid map to the homes of those featured in the pictures.[296] Consider too "Violentacrez," a notorious Reddit administrator

---

[291] Pete Kotz, *Jebidiah Stipe Used Craigslist Rape Fantasy Ad to Get Revenge on Ex-Girlfriend*, TRUE CRIME REPORT (Feb. 9, 2010, 11:13 AM), http://www.truecrimereport.com/2010/02/jebidiah_stipe_used_craigslist.php.

[292] DeeDee Correll, *Craigslist Implicated in Rape Case; A Wyoming Man is Accused of Using the Website to Engineer an Ex-Girlfriend's Assault*, L.A. TIMES, Jan. 11, 2010, at A9.

[293] *Id.*

[294] Caroline Black, *Ex-Marine Jebidiah James Stipe Gets 60 Years for Craigslist Rape Plot*, CBS NEWS (June 29, 2010, 1:29 PM), http://www.cbsnews.com/8301-504083_162-20009162-504083.html; William Browning, *'Terribly Sorry': Craigslist Rapist Receives Same Sentence as Man Who Solicited Assault*, STAR-TRIBUNE (June 30, 2010, 2:00 AM), http://trib.com/news/local/terribly-sorry/article_4b04f85a-21a5-54b5-a3a0-798aa0b8f2bf.html.

[295] Alex Morris, *Hunter Moore: The Most Hated Man on the Internet*, ROLLING STONE, Oct. 11, 2012, at 44, 46–48; Camille Dodero, *Hunter Moore Makes a Living Screwing You*, VILLAGE VOICE, (Apr. 4, 2012), http://www.villagevoice.com/2012-04-04/news/revenge-porn-hunter-moore-is-anyone-up/.

[296] Hill, *supra* note 11; Jessica Roy, *Hunter Moore's 'Scary as Shit' Revenge Porn Site Will Map Submitted Photos to People's Addresses*, N.Y. OBSERVER (Nov. 29, 2012, 8:38 AM), http://betabeat.com/2012/11/hunter-moores-scary-as-shit-revenge-porn-site-will-map-submitted-photos-to-peoples-addresses/. Moore later claimed he had been "drunk" during the interview in which he described the mapping function and would only be posting the addresses of those who attack him. Tracy Clark-Flory, *Hunter Moore: I Lied!*, SALON (Dec. 1, 2012, 8:00 PM), http://www.salon.com/2012/12/02/hunter_moore_i_lied/.

who oversaw forums like "Jailbait," "Creepshots," "Rapebait," "Incest," "Beatingwomen," and "Picsofdeadjailbait," each of which featured pictures and commentary from his followers that celebrated the interests described by the forums' titles.[297]

There is, of course, much more to be written about the incidents and dynamics of cyberharassment crimes. For present purposes, however, the foregoing is sufficient to show that there are significant and legitimate governmental interests at stake in preventing, detecting, and prosecuting various forms of cyberharassment. Although cyberharassment is relatively new, executives and legislatures have manifested these interests by setting up dedicated enforcement units and passing tailored criminal statutes.[298] As we argue in the next section, adopting a mosaic theory of the Fourth Amendment likely will implicate these law enforcement concerns by limiting access to both existing and future digital surveillance techniques and technologies.[299]

C. HOW DIGITAL SURVEILLANCE SERVES GOVERNMENTAL INTERESTS IN PREVENTING, DETECTING, AND PROSECUTING CYBERHARASSMENT

Among the most important methods and strategies used by law enforcement to track and apprehend those who engage in cyberharassment and related crimes are: (1) to identify and track the IP addresses associated with the offending posts and e-mails, (2) to identify and track Media Access Control (MAC) addresses associated with individual computers used in perpetrating these offenses, (3) to use proprietary software to identify the source of images and other files offered through peer-to-peer networks, and (4) to use data screens that monitor Internet traffic for files containing

---

[297] Adrian Chen, *Unmasking Reddit's Violentacrez, the Biggest Troll on the Web*, GAWKER (Oct. 12, 2012, 5:00 PM), http://gawker.com/5950981/unmasking-reddits-violentacrez-the-biggest-troll-on-the-web; David Fitzpatrick & Drew Griffin, *Man Behind 'Jailbait' Posts Exposed, Loses Job*, CNN (Oct. 19, 2012, 11:20 AM), http://www.cnn.com/2012/10/18/us/internet-troll-apology/index.html?hpt=hp_c1.

[298] The federal cyberstalking statute, 18 U.S.C. § 2261A(2)(A) (2006), and state cyberharassment laws criminalize patterns of online behavior that are intended to cause, and do cause, substantial emotional distress. Some states, like New Jersey, have recently passed video voyeur criminal statutes that prohibit "posting a person's sexually revealing recordings or images of victims without their consent if a reasonable person would not have expected to be observed." CITRON, *supra* note 8, at 93. Other statutes include FLA. STAT. ANN. § 784.048 (West Supp. 2013), IOWA CODE § 708.7(1) (2003 & Supp. 2013), MASS. ANN. LAWS ch. 265, § 43A (LexisNexis 2010), VA. CODE ANN. § 18.2-152.7:1 (2009), and S.B. 1411, 2009–10 Leg., Reg. Sess. (Cal. 2010). CITRON, *supra* note 8, at n.134.

[299] Weinstein, *supra* note 118, at 39.

criminal content.[300] In this Part, we explain some of the complications that *Jones* might present with respect to the use of these technologies to identify and prosecute cyberharassers.

Computers connected to the Internet have or share IP addresses. Although the United States has not adopted mandatory data-retention rules like those promulgated by the European Union, ISPs keep records of IP addresses assigned to particular computers at specific times. According to recent reports, major ISPs, such as Verizon and Comcast, generally retain IP addresses from six months to a year.[301] As former Deputy Attorney General Jason Weinstein reported in testimony before the House Subcommittee on Crime, Terrorism, and Homeland Security, these policies are generous by industry standards, but nevertheless may not be long enough to serve many or most law enforcement goals.[302] Let us nevertheless suppose that law enforcement obtains the IP addresses associated with harassing posts within this six-month timeframe. With that information in hand, officials can usually secure the name and account information for the user of that IP address from the ISP that assigned it or from the websites and social networking sites that have been accessed using the identified IP address.[303] If the IP address is permanently or

---

[300] *See* United States v. Budziak, 697 F.3d 1105, 1107–08 (9th Cir. 2012) (describing the Federal Bureau of Investigation's "EP2P" software); United States v. Chiaradio, 684 F.3d 265, 271–72 (1st Cir. 2012) (same); *see also* United States v Gorski, 71 M.J. 729, 731–32 (Army Ct. Crim. App. 2012); United States v. Ahrndt, 3:08-CR-00468-KI, 2013 WL 179326, at *1–3 (D. Or. Jan. 17, 2013); United States v. Broadhurst, 3:11-CR-00121-MO-1, 2012 WL 5985615, at *1–2 (D. Or. Nov. 28, 2012); United States v. Stanley, Crim. No. 11-272, 2012 WL 5512987, at *2 (W.D. Pa. Nov. 14, 2012); Press Release, *supra*, note 245; *Tracking a Troll*, BLITZKRIEG BOPP (Sept. 26, 2012), http://evertb.wordpress.com/2012/09/26/tracking-a-troll/ (describing methods for acquiring and tracking trolls and other posters to internet forums using IP addresses, including the website http://www.iptrackeronline.com/, Google, and AOL's IDP Program).

[301] *How Long Does Your ISP Store IP-Address Logs?*, TORRENTFREAK (June 29, 2012), http://torrentfreak.com/how-long-does-your-isp-store-ip-address-logs-120629/.

[302] *Data Retention as a Tool for Investigating Internet Child Pornography and Other Internet Crimes: Hearing Before the S. Comm. on Crime, Terrorism, & Homeland Sec., H. Comm. on the Judiciary*, 112th Cong. 9 (2011) (statement of Jason Weinstein, Deputy Assistant Attorney General, Criminal Division).

[303] Nate Anderson, *How a Fake Justin Bieber "Sextorted" Hundreds of Girls Through Facebook*, ARS TECHNICA (May 1, 2012, 2:45 PM), http://arstechnica.com/tech-policy/2012/05/how-a-fake-justin-bieber-sextorted-hundreds-of-girls-through-facebook/ (explaining that police tracked a suspect in a sextortion scheme using his IP address, user information provided voluntarily by Facebook, and account information from an ISP); Anderson, *supra* note 285 (outlining how police employed ISP and IP information to track and aprehend a sextortionist who used malware to invade and control his targets' computers); Leo Traynor, *The Day I Confronted My Troll*, GUARDIAN (Sept. 26, 2012, 4:31 AM), http://www.guardian.co.uk/commentisfree/2012/sep/26/day-confronted-troll (describing how he used IP and ISP information to track and identify the troll who harassed

semipermanently assigned to a computer, law enforcement can track its user's online activities more broadly.

Tracing posters through their computers is not always so straightforward a task, of course. Harassers can use public computers in libraries or cafes that do not require registration, limiting traceability through the IP address. In these cases, however, law enforcement agents may be able to use Wifinders and other technologies that can identify individual computers that log onto these open networks by using their MAC addresses.[304] In further efforts to hide their identities, however, harassing posters can employ free and easy-to-use software like Tor, which establishes anonymous Internet connections by funneling Web traffic through encrypted "virtual tunnels."[305] This can make it difficult, if not impossible, to identify IP addresses connected to harassing conduct. Even if posters do not try to hide their identities, their computers may share an IP address with others in a network, which is often the case for universities and workplaces.[306] The IP address would then be of limited help because it could not identify a specific computer on the network. Further complicating matters, some site operators refuse to collect IP addresses from their subscribers at all.

Despite these complications, tracing an IP address is a common and effective way for authorities to identify perpetrators of cyberharassment crimes. At present, the public-observation and third-party doctrines grant law enforcement unfettered discretion to track IP addresses across the Internet. Most cyberharassment is, to one degree or another, public. Furthermore, the third-party doctrine means that law enforcement officers need a subpoena, at most, to secure user information associated with an IP address from ISPs and other third parties, including social-networking sites.[307] A mosaic theory of Fourth Amendment privacy might well change

---

him and his family); Wilson, *supra* note 283 (reporting a case in which police subpoenaed ISPs to locate a suspect in sextortion scheme).

[304] United States v. Ahrndt, 3:08-CR-00468-KI, 2013 WL 179326, at *3–4 (D. Or. Jan. 17, 2013); United States v. Broadhurst, 3:11-CR-00121-MO-1, 2012 WL 5985615, at *1 (D. Or. Nov. 28, 2012).

[305] Paul Bocij & Leroy McFarlane, *Cyberstalking: The Technology of Hate*, 76 POLICE J. 204, 210 (2003) (cataloging encryption software and its uses for criminal activity); *Tor: Overview*, TOR, https://www.torproject.org/about/overview.html.en (last visited May 21, 2013) ("Tor is a network of virtual tunnels that allows people and groups to improve their privacy and security on the Internet. . . . To create a private network pathway with Tor, the user's software or client incrementally builds a circuit of encrypted connections through relays on the network.").

[306] David Robinson, *CCR Symposium: Practical Aspects of IP Logging*, CONCURRING OPINIONS (Apr. 15, 2009, 2:30 PM), http://www.concurringopinions.com/archives/2009/04/ccr_symposium_w.html.

[307] People v. Harris, 945 N.Y.S.2d 505, 507–10 (Crim. Ct. 2012).

all of this. Tracking someone's online activities using an IP address over a period of time is akin to tracking a person through physical space using GPS-enabled tracking devices. By aggregating information about a user and his online activities, law enforcement officers using these fairly basic digital surveillance techniques can therefore assemble precisely the sorts of revealing informational mosaics that worried the concurring Justices in *Jones*.

Digital surveillance technology that offends mosaic sensibilities promises even more benefits than IP traces to law enforcement officers interested in detecting cybercrimes. Take, for example, forums such as those organized and moderated by Violentacrez.[308] Although under current law and free speech doctrine it is perfectly legal to view and comment on pictures of young women in public, law enforcement officers might have reason to worry that habitués of forums like "Jailbait" and "Creepshots" are more likely than most to produce or possess actual child pornography. It is, of course, impossible to conduct even cursory investigations of the tens and hundreds of thousands of those who visit these sites, much less to distinguish between casual curiosity seekers and practicing pedophiles. Here, broad-scale aggregation technology, in combination with ever more sophisticated data analytics designed to identify and track those patterns of online conduct that correlate with higher risks of illegal on- and offline activities, would be tremendously valuable to law enforcement. Once officers have identified a smaller universe of potential offenders, they can then further narrow their investigative fields by using passive techniques like online honey traps to more definitively identify those who are trafficking in or actively seeking to possess child pornography.[309] Again, although these digital surveillance techniques and technologies are not presently subject to Fourth Amendment review, either individually or in the aggregate, the situation would likely change under a mosaic theory. In fact, officers might find themselves assembling informational mosaics sufficient to trigger Fourth Amendment concerns quite by accident.[310] Regardless, law enforcement's legitimate interests in using digital surveillance technology would be affected.[311]

Fusion centers also hold significant potential for law enforcement's efforts to detect and prosecute cyberharassment. The Department of Justice, in conjunction with the National Center for Missing and Exploited

---

[308] Fitzpatrick & Griffin, *supra* note 297.

[309] United States v. Vosburgh, 602 F.3d 512, 517–18 (3d Cir. 2010) (recounting an operation in which the FBI used IP and ISP information to track individuals who attempted to download child pornography from a website operated by the FBI).

[310] Kerr, *Mosaic*, *supra* note 19, at 314–19, 337.

[311] Weinstein, *supra* note 118, at 38–39.

Children, maintains a substantial database of known images of child pornography, each of which has a unique digital fingerprint called a "hash value."[312] Fusion centers, which have access to most Internet traffic, provide a unique—although as yet unexploited—resource that law enforcement agents can use to screen for the transmission of known images of child exploitation. Outside the relatively narrow field of child pornography cases, those who engage in cyberharassment and cyberstalking still tend to use a fairly predictable pattern of words, phrases, and images. The software used by most malicious stalkers also tends to come from a stable of online resources, which again bear an identifiable digital signature. Although the true technical capacities of fusion centers are largely unknown to the public, they appear to have the ability to monitor Internet and communications traffic for precisely these sorts of markers. That same capacity is, of course, precisely what raises concerns about fusion centers from a mosaic theory point of view. Here again, the prospect of adopting a mosaic theory of Fourth Amendment privacy raises serious concerns that the legitimate and important law enforcement goals of detecting and prosecuting cybercrimes may be compromised.

D. STRIKING A REASONABLE BALANCE BETWEEN PRIVACY AND LEGITIMATE GOVERNMENTAL INTERESTS IN PREVENTING, DETECTING, AND PROSECUTING CYBERHARASSMENT

In reflecting on the challenges for citizens, law enforcement officers, courts, and policymakers posed by contemporary calls to limit law enforcement's use of and access to digital surveillance technology, former Deputy Assistant Attorney General Jason Weinstein summed up the stakes:

> So, in considering whether to rewrite the standards that govern law enforcement access to electronic data, policy makers need to consider that choices made out of a desire to enhance privacy may ultimately reduce it, by making it difficult—and in some cases impossible—for law enforcement to pursue the criminals who pose a threat to privacy. More broadly, those choices will have very real consequences for public safety, as they will significantly reduce the ability of law enforcement to investigate and prosecute a wide array of serious crimes.[313]

It is, of course, beyond the scope of this Article to propose specific compromises. Our purpose is, rather, to outline the competing interests and

---

[312] *See Child Victim Identification Program (CVIP)*, NAT'L CTR. FOR MISSING & EXPLOITED CHILDREN, http://www.missingkids.com/missingkids/servlet/PageServlet?LanguageCountry=en_US&PageId=2444 (last visited May 21, 2013); *see also* Press Release, Microsoft, New Technology Fights Child Porn by Tracking Its "PhotoDNA" (Dec. 15, 2009), *available at* https://www.microsoft.com/en-us/news/features/2009/dec09/12-15photodna.aspx (describing the photo analyzing process and the use of hash values).

[313] Weinstein, *supra* note 118, at 39.

to give due weight to the legitimate law enforcement goals at issue. As Judge Posner astutely observed, "[T]he [Fourth] [A]mendment cannot sensibly be read to mean that police shall be no more efficient in the twenty-first century than they were in the eighteenth."[314] With this in mind, the broad outlines of some potential compromises begin to appear.

First, it is important to keep in mind that the interests of law enforcement officers in preventing, detecting, and prosecuting online crimes like cyberharassment and cyberstalking are not antagonistic to the interests of citizens. Neither are they necessarily antagonistic to privacy interests. Rather, as Weinstein points out, consistent and efficient detection and prosecution of these crimes are privacy enhancing, even in the mosaic sense, in that law enforcement success makes online activities safer (and hence less invasive of privacy at the hands of harassers), more accessible, and therefore more useful.[315] This does not mean, of course, that law enforcement officers, engaged in the "often competitive enterprise of ferreting out crime," will not encroach on privacy in the name of preserving it. As the mosaic theory reminds us, perfect security and perfect privacy are mutually exclusive. The challenge, therefore, is to strike a reasonable balance while keeping in mind the fact that law enforcement does not pursue digital surveillance out of prurient interests or a desire to realize some Orwellian dystopia. Rather, their interests are our interests.

Second, achieving a reasonable balance between the various interests at stake in regulating digital surveillance technology under the mosaic theory is unlikely to be a one-size-fits-all affair. In some cases, a warrant requirement may strike the right balance. In other cases, it may be too restrictive. In some cases, prior judicial review of a proposed course of investigation may be required, as is the case now for wiretaps and most searches of homes. In others, post hoc review following the model in place now for most arrests in public may provide sufficient protection of Fourth Amendment rights. Those who design and deploy digital surveillance technologies may also be able to incorporate internal controls that will limit use and access to end users, thereby effecting the reasonable balance of interests required by the Fourth Amendment.[316] The ultimate drivers will, of course, be the interests at stake.

Third, resolving competing interests at stake in a mosaic analysis of

---

[314] United States v. Garcia, 474 F.3d 994, 998 (7th Cir. 2007).

[315] Weinstein, *supra* note 118, at 39.

[316] One prominent government contractor, Palantir, has described its efforts to design software protocols that balance privacy and law enforcement interests in its public documents. *See* PALANTIR TECHNOLOGIES INC., A CORE COMMITMENT: PROTECTING PRIVACY & CIVIL LIBERTIES (2012), *available at* http://www.palantir.com/_ptwp_live_ect0/wp-content/uploads/2012/06/ProtectingPrivacy_CivilLiberties_2012.pdf.

digital surveillance technology will not be a static affair. The fundamental nature of the home and the techniques available to conduct physical searches of homes have changed little since 1791. As a consequence, the solutions developed by courts to contend with physical searches of the home have been fairly stable over time.[317] Digital surveillance is a different matter. The physical, virtual, and social structures of digital spaces are rapidly evolving. So too are the scope and nature of our engagements with digital devices and the intersections between our carbon-constrained and silicon-dependent lives. As the world changes, our reasonable expectations of privacy inevitably will change as well. Digital surveillance technologies are also changing rapidly, providing law enforcement with new tools capable of aggregating and analyzing more and more data from more and more sources. Protecting Fourth Amendment rights in this dynamic environment will require courts, legislators, and law enforcement officials to find a principled, yet flexible, approach to understanding and balancing competing interests.[318]

V. CONCLUSION

The aim of this Article has been to raise questions and issues rather than to answer them. It has certainly not been our goal to offer a comprehensive approach to Fourth Amendment cases after *United States v. Jones*. Rather, our concern here has been to describe some of the most important variables that courts and others interested in securing Fourth Amendment protections under a mosaic theory will need to consider when striking the balance of competing interests that the Fourth Amendment requires. In particular, we have emphasized the important and perfectly legitimate interests of law enforcement officers in using Big Data and digital surveillance technology to prevent, detect, and prosecute two increasingly significant classes of cybercrime: healthcare fraud and cyberharassment. We have also proposed in loose terms a framework that courts and policymakers might employ as they seek both to accommodate the needs of law enforcement and to protect citizens' reasonable expectations of privacy. Among the most important features of that framework is an emphasis on context and adaptability. If the Fourth Amendment is to maintain its role as a bulwark against increasing governmental surveillance while still allowing law enforcement officers to pursue new and evolving forms of criminality in a digital age, then inflexibility and stasis are the true enemies and the surest pathways to unreasonableness.

---

[317] United States v. Jones, 132 S. Ct. 945, 954 (2012).

[318] In other work, we propose just such an approach. *See* Gray & Citron, *supra* note 7.