BIGFOOT:
DATA MINING, THE DIGITAL FOOTPRINT, AND THE CONSTITUTIONALIZATION OF INCONVENIENCE

Carrie Leonetti*

I. INTRODUCTION

"Sometimes I think this whole world is one big prison yard.
Some of us are prisoners, some of us are guards."[1]

A. The Brave New World: The Digital Dragnet

Moore's Law dictates that the number of transistors on a computer processor, and therefore computers' ability to outpace human capacity for processing information, will grow exponentially.[2] The result is that the gap between what human beings and what the computers that they build can do will forever itself increase exponentially.[3] If the Supreme Court does not develop a Fourth Amendment

---

* Carrie Leonetti is an Associate Professor and the Faculty Leader of the Criminal Justice Initiative at the University of Oregon School of Law.

[1] BOB DYLAN, *George Jackson , on* GEORGE JACKSON (Columbia Records 1971).

[2] *See* United States v. Gomez, 807 F.Supp.2d 1134, 1150 n.16 (S.D. Fla. 2011) (stating Gordon Moore's prediction that since the number of transistors per square inch on integrated circuits has doubled every year since its prediction, it is likely that the number will continue to increase in the future); *see also* U.S. DEP'T OF JUSTICE, DOJ INFORMATION TECHNOLOGY STRATEGIC PLAN 2010-2015 7 (2009), *archived at* http://perma.cc/XR7Z-TK7T (stating Moore's law which describes the advancement in computing power per unit cost); NARA Bulletin 2011-02, THE U.S. NAT'L ARCHIVES AND RECORDS ADMIN. (Oct. 10, 2010), *archived at* http://perma.cc/Q9GU-4VDD (discussing the widely recognized distinction between "internet time" and "real time").

[3] *See* Steve Jurvetson, *Transcending Moore's Law with Molecular Electronics and Nanotechnology*, 1 NANOTECHNOLOGY L. & BUS. 70, 71 (2004) (inferring that the

principle that recognizes this exponential potential of computers to intrude on our private lives, the invasiveness of advanced computer technology will eclipse human surveillance as a threat to privacy.[4] Recently, President Obama acknowledged the threat that advancing technology poses to civil liberties, when he noted that "the power of new technologies means that there are fewer and fewer technical constraints on what we can do. That places a special obligation on us to ask tough questions about what we should do."[5]

As Americans now know from the Snowden leak scandal, data mining is already in full swing.[6] Since 9/11, the Government has thrown an enormous amount of resources—agents, money, and computer time—into the "global war on terrorism," which includes tracking suspected terrorists at home.[7] In pursuit of their antiterrorism goals, American law enforcement agencies rely on computer-automated monitoring of phone calls and the Internet, where once agencies had only human intelligence and judgment.[8]

Political parties and commercial retailers also engage in data mining.[9] When people "succumb to that offer for a Walmart gift card or a free iPhone in exchange for taking a survey and divulging all sorts of personal information," such as their addresses, transaction histories, salaries, debt levels, marital statuses, and health histories,

exponential growth of our knowledge of "technical expertise" will lead to a more technology-based society in the future).

[4] *See §2 Computing, Privacy and Freedoms*, INT'L ENCYCLOPAEDIA OF LAWS: CYBER LAW ¶ 408 (2014), *available at* Westlaw 2013 WL 4298923 (stating the potential for computers to threaten human privacy).

[5] Mark Landler & Charlie Savage, *Obama Outlines Calibrated Curbs on Phone Spying*, N.Y. TIMES (Jan. 17, 2014), *archived at* http://perma.cc/P7MA-ZPBN.

[6] *See* Steven Erlanger, *Fighting Terrorism, French-Style*, N.Y. TIMES (Mar. 30, 2012), *archived at* http://perma.cc/HXY2-KGP7 (discussing the automation and computerization of anti-terrorism agencies).

[7] *See id.* (stating how Americans use vast amounts of resources to deal with terrorism).

[8] *See id.* (furthering the contention that computers aid in international anti-terrorism initiatives).

[9] *See* Nicholas Confessore, *Republican Committee Makes Big Turnaround on Fund-Raising*, N.Y. TIMES (Apr. 5, 2012), *archived at* http://perma.cc/U35N-4D5Z (illustrating how the Republican Party recently "revamped its voter database," Voter Vault, which it built during President Bush's tenure in office). The new system allows the targeting and collection of extremely detailed demographic and consumer data on Republican voters. At the same time, the Democrats have invested heavily in information technology and data collection. *See id.*

that information can then be sold to digital marketers.[10] An "incomprehensibly large amount of raw, often real-time data that keeps piling up faster and faster from scientific research, social media, smart phones [and] virtually any activity that leaves a digital trace."[11] Cell phones divulge behavioral and personal information, like phone numbers and in-store browsing habits, to merchants.[12] Companies like Apple, eBay, PayPal, and Amazon record and retain information from users of their mobile payment services.[13] Companies like Google, Facebook, Twitter, YouTube, and Netflix are awash in their users' personal information from their check-ins, geo-tagged photographs, tweets, and movie viewing histories.[14] Facebook, which has amassed more personal data than any other entity in history—names, photos, tastes, and desires of nearly one billion people[15]—now allows its users to buy virtual goods with a currency that it calls Facebook Credits, which "could add transaction histories to its already rich databases of behavioral information."[16]

The Federal Communications Commission recently caught Google operating a surreptitious program that harvested "payload data" user traffic, including the full text of e-mails, passwords, sites visited, and "other sensitive personal information" that was transmitted over unencrypted Wi-Fi networks "from unsuspecting households in the United States and around the world."[17] The program was part of

[10] Nicole Perlroth, *Spam Invades a Last Refuge, the Cellphone,* N.Y. TIMES (Apr. 7, 2012), *archived at* http://perma.cc/C6VP-7QQ4.
[11] Jeanne Carstensen, *Berkeley Group Digs in to Challenge of Making Sense of All That Data,* N.Y. TIMES (Apr. 7, 2012), *archived at* http://perma.cc/8E2J-994K/.
[12] *See* Somini Sengupta, *The New Pay Phone and What It Knows About You,* N.Y. TIMES (Apr. 30, 2012), *archived at* http://perma.cc/P7AC-D7L8 [hereinafter Sengupta, *Pay Phone*] (asserting that cellphone information is monitored and recorded by big business for marketing purposes).
[13] *See id.* (identifying specific corporations, which use cellphone data for online transactions).
[14] *See id.* (comparing corporations that use consumer data).
[15] *See* Somini Sengupta, *Facebook's Prospects May Rest on Trove of Data,* N. Y. TIMES (May 15, 2012) *archived at* http://perma.cc/C2LH-F6HL (declaring that Facebook has obtained massive amounts of consumer data).
[16] *See* Sengupta, *Pay Phone, supra* note 12 (quoting the survey conducted by Chris Jay Hoofnagle, Jennifer M. Urban, and Su Li).
[17] *See* Steve Lohr & David Streitfeld, *Data Engineer in Google Case Is Identified,* N.Y. TIMES (May 1, 2012) *archived at* http://perma.cc/68LC-479Z (outlining Google's efforts to obtain information about customers); *see also* David Streitfeld, *Data Harvesting at Google Not a Rogue Act, Report Finds,* N.Y. TIMES (Apr. 28,

Street View, Google's project to photograph streetscapes over much of the world, which "also involved gathering information about local wireless networks to improve location-based searches."[18] The purpose of the program was to analyze the payload data "offline for use in other initiatives."[19] Perhaps more troubling to privacy advocates,[20] Google's secret data-collection program is not illegal under current American law.[21]

Meanwhile, American intelligence agencies have begun to purchase large corporate databases.[22] The data that the National Counterterrorism Center ("NCTC") is collecting, retaining, and analyzing includes this private commercial data, such as travel records, credit card transactions, e-mail, and phone calls.[23] The data in the Government's possession are so voluminous that it is building massive data centers to house them.[24]

2012), *archived at* http://perma.cc/TD6R-5QQB (explaining the use of "payload data" to advance corporate interests).

[18] Lohr & Streitfeld, *supra* note 17 (describing Google's Street View project).

[19] Streitfeld , *supra* note 17 (stating the intended use of payload data).

[20] *See* Streitfeld, *supra* note 17 (noting privacy advocates found report about data collection troubling).

[21] *See* Streitfeld, *supra* note 17 (noting that Google stated that their data collection was legal).

[22] *See* Siobhan Gorman, Evan Perez & Janet Hook, *U.S. Collects Vast Data Trove*, WALL STREET JOURNAL (June 7, 2013), *archived at* http://perma.cc/ATR8-PA7N (providing an example of a government intelligence agency collecting data from a private company).

[23] *See* Charlie Savage, *U.S. Relaxes Limits on Use of Data in Terror Analysis*, N.Y. TIMES (Mar. 22, 2012), *archived at* http://perma.cc/LJE2-N2GM (describing the government's intrusive collection of data).

[24] *See* James Bamford, *The NSA Is Building the Country's Biggest Spy Center (Watch What You Say)*, WIRED (Mar. 15, 2012), *archived at* http://perma.cc/N6GT-H92P (exposing the government's construction of warehouses used to store large amounts of the public's data—obtained without their knowledge); *see also* Steve Fidel, *Utah's $1.5 Billion Cyber-Security Center Under Way*, DESERET NEWS (Jan. 6, 2011), *archived at* http://perma.cc/9H9B-RGR9 (reporting that the National Security Agency's data center built in Utah cost $1.5 billion); Barton Gellman & Laura Poitras, *U.S., British Intelligence Mining Data from Nine U.S. Internet Companies in Broad Secret Program*, WASH. POST (Mar. 6, 2013), *archived at* http://perma.cc/MFR3-MR2S (affirming the government's priority in collecting public data); Siobhan Gorman, *Meltdowns Hobble NSA Data Center*, WALL ST. J. (Oct. 7, 2013), *archived at* http://perma.cc/NR32-PQU3 (demonstrating that the Utah facility was a massive government construction project). "The Utah facility, one of the Pentagon's biggest U.S. construction projects, has become a symbol of the spy agency's surveillance prowess, which gained broad attention in the wake of

And then, of course, in the summer of 2013, the string of revelations about the National Security Agency (NSA)'s access to and data mining of private information concerning Americans began, with whistleblower Edward Snowden's disclosures about the "Prism" program, which tracks the metadata of Americans' telephone and e-mail communications without meaningful judicial oversight or individualized suspicion.[25] The NSA compiled the data after the FBI obtained orders from the Foreign Intelligence Surveillance Court (FISC) directing telecommunications service providers to produce what it calls "telephony metadata in bulk," which it then handed over to the NSA for storage, search, and analysis.[26]

leaks from NSA contractor Edward Snowden." *Id.*; *see also* Eric Lichtblau & James Risen, *Officials Say U.S. Wiretaps Exceeded Law*, N.Y. TIMES (Apr. 15, 2009), *archived at* http://perma.cc/PV4Z-HSVM (highlighting the government's significant and systemic over collection of domestic correspondence).

[25] *See* ADMIN. WHITE PAPER, BULK COLLECTION OF TELEPHONY METADATA UNDER SECTION 215 OF THE USA PATRIOT ACT 3 (Aug. 9, 2013) [hereinafter WHITE PAPER], *archived at* http://perma.cc/VG33-TZ2U (noting that "information collected includes, for example, the telephone numbers dialed, other session-identifying information, and the date, time, and duration of each call"). The closest thing to an individualized-suspicion requirement in the program (and it is not very close) is a requirement that the metadata collected and analyzed be "relevant to an authorized investigation." *Id.* at 8-9.

[26] *Id.* at 1 (asserting that the "[FISC] first authorized the program in 2006, and it has since been renewed thirty-four times under orders issued by fourteen different FISC judges").

> Under the FISC's orders, the NSA may also obtain information concerning second and third-tier contacts of the identifier (also referred to as "hops"). The first "hop" refers to the set of numbers directly in contact with the seed identifier. The second "hop" refers to the set of numbers found to be in direct contact with the first "hop" numbers, and the third "hop" refers to the set of numbers found to be in direct contact with the second "hop" numbers … Thus, the order allows the NSA to retrieve information as many as three "hops" from the initial identifier.

Id. at 3-4 (explaining how the NSA uses metadata to learn about the associates of callers from terrorist-associated numbers); *see, e.g.*, Conor Friedersdorf, *Admit It, Rep. Sensenbrenner: You Were Wrong About the Patriot Act*, ATLANTIC (June 7, 2013), *archived at* http://perma.cc/Z9VJ-W6YX (explaining that the author of the Patriot Act believes NSA is using overbroad interpretation and threatening Americans' constitutional rights); Landler & Savage, *supra* note 5 (balancing the need for broad surveillance and the need for privacy based restrictions); James Risen & Laura Poitras, *Spying by N.S.A. Ally Entangled U.S. Law Firm*, N.Y. TIMES, (Feb. 16, 2014) [hereinafter Risen & Poitras, *U.S. Law Firm*], *archived at* http://perma.cc/QC8L-GSZF (quoting that "justifying the NSA's sweeping powers,

The NSA also intercepts the communications of Americans if they are in contact with a foreign intelligence target abroad.[27] Disclosures in recent months from Snowden's leaked documents show that the agency routinely spies on trade negotiations, the communications of economic officials in other countries, and foreign corporations.[28] The most recent revelations now show that these data-collection practices intended to target foreign suspects have included monitoring an American law firm representing a foreign government in trade disputes with the United States.[29]

B. The Constitutional Dilemma

All of these various intersecting projects overlap to authorize domestic law-enforcement and intelligence agencies to collect information about Americans on a far greater scale than may be suggested by any single authorization alone.[30] When these searches are done without a warrant, they have significant impacts on privacy.[31] In the meantime, advances in technology are rapidly outpacing the state of the law.[32]

This Article focuses on one subset of these searches: warrantless data mining. Whether these warrantless searches count as searches for Fourth Amendment purposes and whether they fit within an exception to the general warrant requirement are unresolved ques-

---

the Obama administration often emphasizes the agency's role in fighting terrorism and cyberattacks …").

[27] *See* Risen & Poitras, *U.S. Law Firm*, *supra* note 26 (explaining how although the NSA is prohibited from targeting Americans, they are permitted to receive information if an American citizen is in contact with a foreign intelligence target).

[28] *See* Risen & Poitras, *U.S. Law Firm*, *supra* note 26 (describing how agency information was critical to many departments, for example the Agriculture Department).

[29] *See* Risen & Poitras, *U.S. Law Firm*, *supra* note 26 (noting that the NSA may collect data for its own intelligence purposes, including attorney client privileged information).

[30] *See infra* Part I.A (summarizing how certain government agencies are able to collect information concerning American citizens).

[31] *See* Katz v. United States, 389 U.S. 347, 358-59 (1967) (addressing the requirement for search warrants to begin surveillance of a telephone booth and stating "[w]herever a man may be, he is entitled to know that he will remain free from unreasonable searches and seizures").

[32] *See* Risen & Poitras, *U.S. Law Firm*, *supra* note 26 (noting that the American Bar Association recommended changing ethics rules due to growing concerns about surveillance and hacking).

tions because the Supreme Court has not weighed in on them.[33] Unless the Government uses the data that it has mined as evidence against a particular individual (or unless a Government whistleblower is willing to risk international extradition and federal prison), people generally are not even aware that the data mining has occurred and, thus, are not in a position to challenge it in court.[34]

Government data mining poses a conundrum for current Fourth Amendment jurisprudence.[35] Its individual components (records and the individual items of information – consumer purchases, public surveillance, information contained in public records) are all legal for the Government to acquire, without a warrant or probable cause, individually.[36] All of the individual points of information being analyzed are available already.[37] But the individual information is of little use in criminal investigations.[38]

The investigatory contribution of new data-mining technologies is the Government's ability to collect, combine, and analyze them in the aggregate: to make a computer database with every piece of information about every person and conduct "pattern analyses" of it.[39] It is only the collection and aggregation of millions of these individual data points by modern computers that gives the items mean-

[33] *See* Hedrick Smith, *Pre-emption & the Fourth Amendment*, FRONTLINE PBS, *archived at* http://perma.cc/7FAM-M6ZU (describing how the use of data mining can create Fourth Amendment issues in regard to the protection of civil liberties); *NSA Spying FAQ*, ELECTRONIC FRONTIER FOUNDATION, *archived at* http://perma.cc/X45A-XA6W (arguing how lawsuits about data mining give rise to specific legal claims including Fourth Amendment concerns).

[34] *See* Smith, *supra* note 33 (alleging that the government's massive data mining is unknown to the majority of Americans).

[35] *See* Christopher Slobogin, *Government Data Mining and the Fourth Amendment*, 75 U. CHI. L. REV. 317, 321 (2008) (explaining that "Fourth Amendment jurisprudence appears to leave data mining completely unregulated").

[36] *See Data Mining, Dog Sniffs, and the Fourth Amendment*, 128 HARV. L. REV. 691 (Dec. 2014) (noting that "[t]he Supreme Court has held that one cannot have a reasonable expectation of privacy in information that is given to third parties or made accessible to the public").

[37] *See* Streitfeld, *supra* note 17 (noting that the Federal Communications Commission found no law was broken when engineer collected unencrypted data while working on Google's Street View project).

[38] *See* Streitfeld, *supra* note 17 (commenting on how an engineer invoked his Fifth Amendment protection against self-incrimination and in doing so left many unanswered questions about data collection).

[39] *See* Slobogin, *supra* note 35, at 323 (explaining how pattern analysis is used in data mining to advance national security).

ing and the Government the ability to profile its citizens without oversight from the courts – what one court has referred to as the "mosaic" resulting from "a broad view of the scene."[40]

The Government has defended the warrantless data mining on the ground that it is tracking only *metadata* (data about phone conversations, like cell-phone locations, the identities of parties to communications, dates and times of communications) rather than the *contents* of telephone calls and e-mails—in other words, who is communicating, when, where and with whom, but not what is being communicated.[41] In a recent case, the United States Court of Appeals for the Sixth Circuit agreed, holding that, even after *United States v. Jones*,[42] "pinging" a cell phone did not infringe on its user's reasonable expectation of privacy in his/her location.[43] This distinction, however, between metadata (date, time, phone numbers, location) and contents (the conversation itself) is a shallow one.[44]

Imagine, for a minute, attempting to get through an average day without leaving an electronic trace. When you wake in the morning, do not turn on your cell phone or any other device with global

[40] *See* United States v. Maynard, 615 F.3d 544, 562 (D.C. Cir. 2010) (describing how the harvested data is made useful through the use of the mosaic theory).

[41] *See, e.g.*, WHITE PAPER, *supra* note 25, at 1 (stating "[t]his information is limited to telephony metadata, which includes information about what telephone numbers were used to make and receive the calls, when the calls took place, and how long the calls lasted. Importantly, this information does *not* include any information about the content of those calls"). This is in contrast to its prior defense of the NSA's warrantless wiretapping of the *contents* of international telephone calls on the ground, inter alia, that such searches were justified under the special-needs doctrine. *See* U.S. DEPT. OF JUSTICE, LEGAL AUTHORITIES SUPPORTING THE ACTIVITIES OF THE NATIONAL SECURITY AGENCY DESCRIBED BY THE PRESIDENT 40-41 (Jan. 19, 2006) (supporting the contention that the government only uses data retrieval for megadata and not content based).

[42] 132 S. Ct. 945, 949 (2012) (holding that long-term GPS tracking of Jones' car was considered a search and thus within the province of the Fourth Amendment).

[43] *See* United States v. Skinner, 690 F.3d 772, 777-78 (6th Cir. 2012) (holding that pinging a cell phone does not violate the Fourth Amendment); *see also* United States v. Stokes, 733 F.3d 438, 441 n.3 (2d Cir. 2013) (explaining that "Pinging" a cell phone allows officers to gather data on the phone's physical location); United States v. Barajas, 710 F.3d 1102, 1104-05 (10th Cir. 2013), *cert. denied*, 134 S.Ct. 230 (2013) (illustrating how DEA agents engaged in wiretap surveillance and GPS pinging of cell phones).

[44] *See* Stilgherrian, *Metadata and Content: a distinction without difference*, CRIKEY (2014), *archived at* http://perma.cc/U94E-2K2U (referencing research that shows that distinction between meta-data and content is minute).

positioning satellite ("GPS") location services (or your phone company will know where you are). Do not use anything that runs off of electricity (or your electric company will know that you are home). Do not arm your burglar alarm (or your alarm company will know when you leave). Do not drive in your car (or your car's computer will record driving information for use if you have a car accident). Avoid public cameras that could be mined for facial recognition information (ATMs, convenience stores, public transportation hubs). Do not use a credit or debit card or withdraw money from your bank account (or the bank will know that you have done so, where, and how much you have withdrawn). Do not talk on the telephone or send a fax or e-mail (or your phone company or ISP will know that you have done so). Obviously, no Facebook or Instagram. Do not use your pass card to go to the gym, park a car, or go to work after hours.

Most of us do not care if our bank knows that we have withdrawn $100 or used a debit card to buy a croissant and latte. On the contrary, we hope that they are keeping an eye on our withdrawals and purchases as the stewards of our financial transactions and assets. In fact, unless we are contemplating a crime spree, most of us do not care about revealing any of the individual items of information being protected in the hypothetical above – and that is the point. We lack a subjective expectation of privacy in them, and probably even lack a reasonable objective expectation of privacy in them.

Now, imagine that you ignored my advice and did all of those things. And imagine that your utility companies, ISPs, local businesses, and employers sold *all* of that information to the Government (or provided it in response to a third-party subpoena) – not the contents of the communications, of course, but merely the metadata – the time, duration, and location of your actions and the identities of those with whom you performed them. Imagine further (because it is possible), that the Government built a profile of you from it: on Wednesdays, Carrie gets up around 7:00 (burglar alarm off, energy usage increases), checks her e-mail and posts on Facebook for fifteen minutes (ISP and Facebook data), leaves her house around 7:30 (burglar alarm on, car moving), goes to the gym for forty-five minutes (parking pass, gym card swipe), then to work (car data storage, parking pass, building entrance pass, computer activity), where she talks on her phone for half an hour to her grandmother (cell phone records),

who is not a United States citizen (DHS records).[45] The government's resulting picture of your day—your activities, your communications, your companions—would be far more detailed than the picture anyone in your life—partner, child, parent—would have.

Now imagine that one day you varied your routine. Maybe you were playing hooky from work; maybe you were having an extramarital affair; maybe you were plotting an act of civil disobedience with a radical political group. No matter the reason, the first person who would know is the FBI computer analyst watching for patterns in your aggregate data: bothered yet?

This is the conundrum of data mining. Individually, it involves data points, usually metadata, taken from activities that we knowingly share with others because we have no interest in hiding them.[46] Collectively, it confers the ability to track our every move, but only because computer technology permits organizations (the NSA, the FBI, Walmart) to do so.[47] The Government has conceded as much in its defense of the Prism metadata collection program: "[C]ommunications metadata is different from many other kinds of records because it is inter-connected and the connections between individual data points, which can be reliably identified only through analysis of a large volume of data, are particularly important to a broad range of investigations of international terrorism."[48] The question that this Article seeks to answer is seductively simple: what is the difference?[49] Do data in the aggregate invade our privacy in a way that data points individually do not and, more importantly, do they do so in a way that is constitutionally cognizable under the Fourth Amendment?[50] Is the act of mining large volumes of metadata with the assistance of powerful computers—the ability of comput-

[45] *See* Lindsay Wise & Jonathan S. Landay, *Government Could Use Metadata to Map Your Every Move*, MCCLATCHY WASHINGTON BUREAU (2013), *archived at* http://perma.cc/4CUF-V98J (suggesting that it is possible to build a profile on an individual based on meta data gathered from their everyday activities).
[46] *See id.* (providing an example of the information that can be mined from a tweet).
[47] *See id.* (stating that computer technology is advanced enough to allow organizations to analyze data to expose patterns).
[48] WHITE PAPER, *supra* note 25, at 2.
[49] *See* WHITE PAPER, *supra* note 25, at 2 (asking the difference between metadata in bulk versus other types of data).
[50] *See* WHITE PAPER, *supra* note 25, at 2 (framing the question discussed in this article).

ers to aggregate data that no mere mortal ever could—somehow greater than the sum of its parts?

The central problem presented by data mining is that, in the pre-digital age, most of the information privacy that people enjoyed did not arise from legal or constitutional limitations on searches and seizures of information.[51] It was the result simply of the lack of technology to amass these large stores of information and analyze them with computer algorithms to create detailed personal information profiles of all Americans. Our protection was feasibility, not constitutionality.[52] But with the advent of Big Data, it is now possible to amass an enormous amount of personal information about people from individual items of information knowingly exposed only as single data points.[53]

This Article posits that the sheer volume of information that the Government can now collect on Americans (in the absence of individualized suspicion and the sophisticated algorithms that it uses to aggregate and analyze it) raises independent privacy concerns that themselves should trigger Fourth Amendment protections.[54] Data mining makes readily available information that would otherwise be difficult to obtain.[55] The lack of meaningful restrictions on who can access mined data or whom the Government can target in its collection and analyses means that the data are available regardless of the existence of suspicion of wrongdoing, their materiality to an ongoing investigation, or their subsequent use.[56] The breadth of information and extent of access all but eliminates the possibility of privacy for all of us whose data are being mined.[57]

---

[51] *See* Transcript of Oral Argument at 43-44, 60, United States v. Jones, 132 S. Ct. 945 (2011) (No. 10-1259) *archived at* http://perma.cc/LUD3-XQS7 (transcribing Justice Alito's point about the distinction between live surveillance and GPS tracking during the oral arguments in *Jones*).

[52] *See id.* (explaining technological advancements and their impact on security).

[53] *See id*. at 10-11 (describing the vast data collection capabilities of modern technologies).

[54] *See contra Data Mining, Dog Sniffs, and the Fourth Amendment*, *supra* note 36 (contrasting the argument that data mining falls within the fourth amendment).

[55] *See* Wise & Landay, *supra* note 45 (exemplifying the advancement in data mining capabilities resulting in more intrusion in our daily lives).

[56] *See* Wise & Landay, *supra* note 45 (describing a lack of restrictions on data mining).

[57] *See §2 Computing, Privacy, and Freedoms*, *supra* note 4 (indicating that inadequate restrictions on data mining result in significant loss of privacy).

II. SEARCH PARTY: CURRENT UNDERSTANDINGS OF THE REASONABLE EXPECTATION

A. Basic Principles: the Meaning of "Search"

The touchstone for the question presented by this Article, as in all Fourth Amendment inquiries, is Justice Harlan's two-part test in *Katz v. United States*.[58] Justice Harlan's test dictates that the proper focus of any inquiry into the existence of a search (the trigger point for any Fourth Amendment protection) is the reasonableness of the expectations of privacy of the individuals affected by the Government's invasions.[59] In simplest terms, the question is whether individuals who wish to "opt out" of Government data mining and profiling are reasonable in their expectation that their wishes will be respected in the absence of a judicial warrant and probable cause supporting it.[60] This question can be divided into an empirical (majoritarian) and a normative question.[61] Do most Americans think that the Government is violating their privacy when it mines and analyzes their personal data and, if so, should they?[62]

In general, in answering those questions, courts tend to look to factors like the possessory or property interest that individuals

---

[58] *See Katz*, 389 U.S. at 361 (Harlan, J., concurring) (explaining Justice Harlan's "twofold requirement"). Katz was convicted of transmitting wagering information over a public telephone, in violation of the federal wire-fraud statute. The police obtained the evidence to convict him by electronically eavesdropping, without a warrant, on the public pay phone that he used to place bets. *See id.* at 348-50.

[59] *See id.* at 361 (explaining how the Court has subsequently adopted Justice Harlan's test, from his concurring opinion in *Katz*, in all Fourth Amendment cases); Smith v. Maryland, 442 U.S. 735, 740 (1979) (affirming the twofold requirement used in *Katz*).

[60] *See Smith*, 442 U.S. at 741 (applying the *Katz* analysis to issue of whether the Government infringed a "legitimate expectation of privacy" in absence of a judicial warrant).

[61] *See id*. at 740 (noting the questions in *Katz* on whether the individuals actions displayed an actual expectation of privacy (empirical) and whether the public wishes to enforce that expectation (normative)).

[62] *See Majority View NSA Phone Tracking as Acceptable Anti-terror Tactic*, PEW RESEARCH CENTER (June 10, 2013), *archived at* http://perma.cc/4LF9-UHUH (reporting that the majority of Americans believe that telephone tracking is acceptable when investigating terrorism). However, the article is silent on other potential law enforcement uses of tracking data. *See id.*

have in the private area invaded (their daily activities),[63] longstanding social customs, practices, and expectations (our social contract governing cyber surveillance), the relation of the area invaded (trackable human activity) to illegal activity, the setting in which the activity occurs (in this case, sometimes in the sanctity of the home, sometimes in the public square, and sometimes in the Neverland of the Internet in between), assumption of risk (whether one assumes a risk of tracking by virtue of having credit cards, a Facebook page, utility accounts, or interacting with businesses), vantage point (FBI or NSA headquarters, via the Internet), and whether there has been any trespass or physical intrusion into a protected area (e.g., by retrieving the data off of the suspect's home computer rather than from third parties).[64]

Although the Court in *Katz* declared that the Fourth Amendment protected "people, not places," the setting in which government action takes place is nevertheless one of the most important factors in determining the existence of a "search" or "seizure."[65] For example, in *California v. Ciraolo,* the Court found that Ciraolo's backyard marijuana garden was in plain view when officers spotted it from a helicopter 1,000 feet overhead in part because he had not taken sufficient steps to shield it from public view (in navigable airspace), which also diminished the reasonableness of any expectation of privacy that Ciraolo may have had in his yard.[66] The Court's recent decision in

[63] *See, e.g.*, United States v. Jacobsen, 466 U.S. 109, 113 (1984) (explaining that the collection of physical evidence constitutes a "seizure" for Fourth Amendment purposes when it causes a meaningful interference with an individual's possessory interests in the property collected).

[64] *See id*. at 136-37 (explaining that a large number of investigative techniques are not regarded as either a "search" or a "seizure" under Fourth Amendment analysis and do not require a warrant or probable cause). However, before a class of investigative techniques are excluded, the courts require certainty that protected areas of personal security and privacy are not threatened. *See id.*

[65] *See Katz*, 389 U.S. at 351 (noting that "what a person knowingly exposes to the public . . . is not a subject of Fourth Amendment protection" but one does not "shed his right" to privacy by making a telephone call in a place where he can be *seen* by the public).

[66] *See* California v. Ciraolo, 476 U.S. 207, 209 (1986) (providing summary of facts); *see also id. at* 213-15 (explaining the Court's view of reasonable expectation of privacy under the Fourth Amendment); Note, *supra* note 36, at 691 (highlighting the Fourth Amendment issues with data mining); *Katz*, 389 U.S. at 373 (Black, J., dissenting) (stating that Fourth Amendment privacy only protects to the extent that it prohibits unreasonable searches and seizures or persons, houses, papers, and ef-

Florida v. Jardines is also exemplary of this process.[67] In *Jardines*, police officers used a drug-sniffing dog on the front porch of Jardines's home to follow up on a tip that he was cultivating marijuana inside.[68] The Court held that the police violated Jardines's Fourth Amendment rights because they didn't have a warrant when they invaded the curtilage of Jardines's home.[69]

B. The State-Action Requirement

Another confounding requirement, when applied to data mining, is the state-action question: when the Government mines data voluntarily disclosed by individuals (e.g., consumers) to nongovernmental sources (e.g., corporate retailers), even if there is a search, who is conducting it? In other words, even if some part of the data-mining process is a "search" as the Fourth Amendment defines that term, which part – the gathering (done mostly by private third-party entities) or the aggregation and analysis (done by the Government)? If the answer is the former (the private action of first-line collection), then, under *Skinner v. Railway Labor Executives' Ass'n*[70] and *Burdeau v. McDowell*,[71] the Fourth Amendment cannot regulate data mining, unless, by purchasing at least some of the data, the Government can somehow be deemed to be soliciting its collection.[72] This is

fects.); Florida v. Jardines, 133 S. Ct. 1409, 1413 (2013) (discussing the Court's reliance on trespass theory to invalidate the dog sniff at issue).

[67] *See Jardines*, 133 S. Ct. at 1413 (exemplifying the Court's definition of a traditional search for Fourth Amendment purposes).

[68] *See id*. at 1413 (explaining the facts of the case).

[69] *See id.* at 1417-18 (explaining the application of Fourth Amendment on issues involving curtilage)*; see also* Carrie Leonetti, *Open Fields in the Inner City: Application of the Curtilage Doctrine to Urban and Suburban Areas*, 15 GEO. MASON U. C.R. L.J. 297, 298-303 (2005) (detailing the history of the curtilage doctrine).

[70] *See* Skinner v. Ry. Labor Execs.' Ass'n, 489 U.S. 602, 614-15 (1989) (holding that Government compulsion renders a private actor an instrument or agent of the Government for the purpose of determining whether the searches that such actor conducts constitute government action for Fourth Amendment purposes).

[71] *See* Burdeau v. McDowell, 256 U.S. 465, 475 (1921) (holding that the Fourth Amendment only protected against unlawful searches and seizures by the Government and that it was not violated by the seizure of private papers by a private corporation from the possession of an employee, even when such seizure was unlawful).

[72] *See id.* at 475 (explaining that "[t]he Fourth Amendment gives protection against unlawful searches and seizures, and as shown in the previous cases, its protection applies to governmental action").

an unpersuasive argument because private entities surely collect data for other reasons, like product fulfillment, billing, fraud detection and prevention, and legal compliance.[73] Furthermore, not only is the Government not involved in the invasion of collecting the data, the collection probably is not an "invasion" at all, since most of us willingly reveal to Facebook and its audience what we post on our walls.[74] To pose a constitutional problem, there must be something in the aggregation and analysis of the data itself that is an invasion, since that is where the Government action in these cases lies.

Adding to this conundrum is President Obama's recent proposal that the large stores of collected data be maintained by private entities, like phone companies and internet service providers, rather than by government agencies directly.[75] This suggestion implies that at least the President believes that the Government's mining of private data held by third parties would be less constitutionally objectionable than the NSA or FBI storing the data itself.[76] This suggestion is also based on the assumption that the act of mining and analyzing the data is not a search, but instead that only the initial collection of the data is.[77]

C. Data Mining & the Plain View Doctrine

One prominent exception to the Fourth Amendment's general requirement that police conduct searches and seizures only pursuant to a judicial warrant issued on the basis of probable cause is when the

[73] *See, e.g.*, United States v. Miller, 425 U.S. 435, 443 (1976) (explaining third party doctrine). "This Court has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed." *Id.*

[74] *See* Sengupta, *supra* note 15 (discussing that many Facebook users post personal data online that the public can see).

[75] *See* Landler & Savage, *supra* note 5 (reporting that President Obama's speech outlined only suggested principles, leaving the details to Congress and the Department of Justice).

[76] *See* Landler & Savage, *supra* note 5 (suggesting that the government stop storing collected data, and seek court approval in all but emergency cases to access third party data for analysis).

[77] *See Katz*, 389 U.S. at 351 (stating that a person does not have a reasonable expectation of privacy when they expose the information they wish to protect to the public).

item searched or seized is already in "plain view" at the time of its search and/or seizure—and its related corollaries: plain smell, plain feel.[78] While this exception historically has applied to the canonical case of drugs seen through the open front window or the gun seen through the windows of an automobile during a traffic stop, it is not limited to contraband in plain view in a physical area.[79] When individuals knowingly expose digital information—for example, data about their location and activities—to third parties, they have arguably placed it in "plain view" such that its search and seizure by law-enforcement officers does not require a warrant and probable cause, as long as the officers were legally in the location (or database) at the time that they observed (or obtained and analyzed) it.[80] In this way, the plain-view doctrine often collapses back into the *Katz* test for searches, because when one knowingly exposes his/her information to a third party (places it in "plain view"), one also likely loses any reasonable expectation of privacy therein.[81]

III. TECHNOLOGY & A UNIFIED THEORY OF PRIVACY

[78] *See* Harris v. United States, 390 U.S. 234, 236 (1968) (holding that when a police officer has the legal right to be where they are, objects or activities occurring within plain view may be introduced into evidence); United States v. Place, 462 U.S. 696, 707 (1983) (declaring that the exposure of a police dog to a person's luggage which was located in a public place did not constitute a warrantless search).

[79] *See, e.g.*, *In re* Application of U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to Gov't, 620 F.3d 304, 319 (3d Cir. 2010) (holding that the Government did not need a warrant to require a cellular service provider to produce a customer's location history, but may obtain a court order showing "specific and articulable facts" establishing a reasonable belief that the information sought is "relevant and material" to an ongoing investigation).

[80] *See Katz*, 389 U.S. at 361 (Douglas, J., concurring) (highlighting that activities or statements exposed to the "plain view of outsiders" are not protected).

[81] *See Katz*, 389 U.S. at 351 (dictating that whatever a person knowingly exposes to public view, even in their own home or office, is not private); Washington v. Chrisman, 455 U.S. 1, 2 (1982) (holding that under the Fourth Amendment, an officer lawfully in a student's dorm room could seize marijuana seeds and a pipe that were in plain view); Hester v. United States, 265 U.S. 57 (1924) (the Fourth Amendment protection does not extend to open fields because they are public areas); People v. Hines, 260 Cal. App. 2d 13, 17 (1968) (finding no search and seizure and "[o]bserving things which are open to view does not constitute a search").

Katz relies upon evolving constitutional values.[82] Although Fourth Amendment jurisprudence has generally found that individuals lack a reasonable expectation of privacy in their activities that occur in (or are made) public, invasive technology can change the calculus.[83] The Court has indicated a willingness to distinguish high- and low-tech searches in a few contexts.[84]

A. Home is Where the Heat Is: Thermal Imaging & Other Sensory Enhancement

One is in the use of sensory enhancement devices like thermal imagers.[85] In *Kyllo*, the Court held that police use of a thermal imager to detect marijuana "grow lamps" within a home was a search, even though such search did not involve a "physical intrusion" into the home, although it limited its holding to technology that was "not in general public use" and to high-tech surveillance of the interior of a home, in particular.[86] The Court rejected the alternative test proffered by the dissent—whether a new technology offered the functional equivalent of actual police presence in the area being searched—as inadequate to protect privacy.[87]

The Court's reasoning, while limited to thermal imaging of the home, bears on the pattern detection that data mining makes pos-

[82] *See Katz*, 389 U.S. at 351 (referring to protection against unreasonable searches and seizures as guaranteed by the Fourth Amendment).
[83] *See* Kyllo v. United States, 533 U.S. 27, 34 (2001) (addressing the limits on the power of technology and how it limits the guaranteed privacy granted under the Fourth Amendment).
[84] *See Katz*, 389 U.S. at 352 (referencing cases in which Fourth Amendment protection applies, such as "in a business office, in a friend's apartment, or in a taxicab").
[85] *See Kyllo*, 533 U.S. at 33 (concluding that "[i]t would be foolish to contend that the degree of privacy secured to citizens by the Fourth Amendment has been entirely unaffected by the advance of technology").
[86] *See id.* at 29-30 (where agents used a thermal-imaging device to scan a home to determine if an abnormally large amount of heat was emanating from it, which would have been consistent with the high-intensity lamps typically used for indoor marijuana growth); *see also id.* at 30 (finding that "[t]he scan showed that the roof over the garage and a side wall of petitioner's home were relatively hot compared to the rest of the home and substantially warmer than neighboring homes in the triplex," and further reasoning that based in part to the thermal imaging, agents obtained a warrant to search Kyllo's home, where they found marijuana growing).
[87] *See id.* at 39 (determining that "[t]he dissent offers no practical guidance of the application of this standard, and for reasons already discussed, we believe there can be none").

sible.[88] The Court reasoned that obtaining by sense-enhancing technology information regarding a home's interior that could not otherwise have been obtained without physical intrusion constituted a search and rejected as "mechanical" the Government's argument that individuals lacked a reasonable expectation of privacy in the amounts of heat radiating from their homes.[89] The Court specifically noted that the case "involve[d] officers on a public street engaged in more than naked-eye surveillance of a home."[90] The Court expressed the concern that permitting warrantless thermal imaging would leave the homeowner at the mercy of advancing technology—including imaging technology that could someday discern all human activity in the home.[91] In *Kyllo,* the Court vindicated what it termed the principle of "otherwise-imperceptibility."[92]

For several years, *Kyllo* was something of an outlier among the current Court's Fourth Amendment jurisprudence, a seemingly anomalous occasion in which the Court was willing to use the *Katz* test to invigorate privacy protections for activities that could be monitored without a physical intrusion into a constitutionally protected area.[93]

B. "The Sum of the Parts:" Regulation of GPS Tracking Devices

More recently, however, the Court has shown a willingness to distinguish high- and low-tech surveillance in the context of GPS

[88] *See id*. at 35 (upholding thermal imaging because it detected "only heat radiating from the external surface of the house").
[89] *See id.* at 35-6 (opining that reversing that approach would endanger the Fourth Amendment protections).
[90] *Id.* at 33.
[91] *See Kyllo*, 533 U.S. at 35-36 (distinguishing the fundamental difference between what the dissent refers to as "off-the-wall" observations and "through-the-wall surveillance").
[92] *See id.* at 38 n.5 (relying on the distinction between invasive modern technology that would reveal "those intimate associations, objects or activities otherwise imperceptible to police or fellow citizens").
[93] *See, e.g., Ciraolo,* 476 U.S. at 215 (holding that visual observation from public navigable airspace was not a search); Dow Chemical Co. v. United States, 476 U.S. 227, 240 (1986) (Powell, J., concurring in part and dissenting in part) (holding that enhanced visual surveillance via aerial photographs from public navigable airspace was not a search).

tracking devices.[94] In 1983, in *Knotts*, the Supreme Court held that the police planting a beeper in a can of chloroform,[95] which was then placed in a vehicle and used to monitor the car's movements on public roads,[96] was not a search within the meaning of the Fourth Amendment.[97] Knotts argued that permitting the warrantless use of the beeper was tantamount to approving "twenty-four hour surveillance of any citizen of this country… without judicial knowledge or supervision."[98] The Court rejected Knotts's argument, explaining:

> [I]f such dragnet-type law enforcement practices as respondent envisions should eventually occur, there will be time enough then to determine whether different constitutional principles may be applicable. . . . Insofar as respondent's complaint appears to be simply that scientific devices such as the beeper enabled the police to be more effective in detecting crime, it simply has no constitutional foundation. We have never equated police efficiency with unconstitutionality, and we decline to do so now.[99]

The Court applied this principle to hold that the police did not need a warrant to use the radio beeper to assist them in tracking the vehicle as it traveled over the public roadways.[100] The Court reasoned that a person "traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place

---

[94] *See* United States v. Knotts, 460 U.S. 276, 281 (1983) (equating the use of a radio beeper to the low-tech method of visual surveillance conducted by police following an automobile).

[95] *See id.* at 278 (noting that chloroform is a chemical precursor to the manufacture of some illicit drugs).

[96] *See id.* (stating that police placed a beeper in a five-gallon drum of chloroform with the consent of the manufacturer, and used the signal from that beeper to locate a clandestine drug lab at a cabin owned by Knotts).

[97] *See id.* at 285 (holding that police monitoring of the beeper signal from the chemical drum did not violate a legitimate expectation of Knotts's privacy, and thus "was neither a 'search' nor a 'seizure' within the contemplation of the Fourth Amendment").

[98] *Id.* at 283.

[99] *Id.* at 284.

[100] *See Knotts*, 460 U.S. at 281-82, 285 (asserting that a person driving on a public street has no reasonable expectation of privacy, and that the use of a beeper for surveillance in this instance is equivalent to following a vehicle on a public roadway).

to another."[101] In other words, the Court decided that motorists cannot reasonably expect their movements on public roads to remain private.[102]

Based on *Knotts*, it stood to reason that warrantless electronic tracking was constitutionally permissible, as long as it involved movements on public roads.[103] At the time that the Court decided *Knotts*, however, the idea of the police flipping on a computer and using a satellite in outer space to track a suspect's car in real-time would have been science fiction.[104] But today, by attaching a device no bigger than a book of matches to a car without the driver's knowledge, the police can watch and record all of the vehicle's travels on public roads, twenty-four hours per day, on a laptop.[105] Over the past three decades, many state and federal courts have applied the Supreme Court's rationale in *Knotts*, holding that GPS monitoring is not a 'search' that requires a warrant and probable cause.[106]

---

[101] *Id.* at 281.

[102] *See id.* at 281-82 (describing travel over public streets as a voluntary conveyance of one's travel to any interested onlooker).

[103] *See id.* at 281-82, 285 (holding that warrantless use of a radio beeper in tracking a drum of chloroform to the Respondent's residence did not violate the Respondent's Fourth Amendment rights because the driver of the vehicle had no expectation of privacy while on a public thoroughfare).

[104] *See* Mark Sullivan, *A Brief History of GPS*, TECHHIVE (Aug. 9, 2012), *archived at* http://perma.cc/Y2JF-88S5 (outlining the timeline of GPS development, specifically noting that the U.S. military completed installation of the suite of 24 satellites that make up the GPS system in 1995).

[105] *See* Justin Scheck, *Stalkers Exploit Cell Phone GPS*, WALL ST. J. (Aug. 3, 2010), *archived at* http://perma.cc/377N-WXDF (discussing how GPS technology installed in mobile phones is commonly used to establish an individual's location, and some of the users of this technology are police).

[106] *See, e.g.*, United States v. Forest, 355 F.3d 942, 950 (6th Cir. 2004) (holding, based on *Knotts*, that Forest had no legitimate expectation of privacy under the Fourth Amendment in his location or in his cell phone data that DEA agents obtained by calling him and used to track his location on public highways, notwithstanding that the agents were unable to maintain visual contact with his car without them); *see also* United States v. Jones, 31 F.3d 1304, 1309 (4th Cir. 1994) (holding, based on *Knotts*, that postal inspectors' use of an electronic tracking device to monitor the contents of Jones's van was not an illegal search); United States v. Butts, 729 F.2d 1514, 1517 (5th Cir. 1984) ("*Knotts* teaches us here that monitoring signals from an electronic tracking device that tells officers no more than that a specific aircraft is flying in the public airspace does not violate any reasonable expectation of privacy. Because this is so, no Fourth Amendment violation results from such public detection. The movement of an airplane in the sky, like that of an automobile on a highway, is not something in which a person can claim a reasonable

Recently, however, in *United States v. Jones*,[107] the Supreme Court disagreed, at least under the limited facts of the case.[108] In *Jones*, the police had engaged in the high-tech surveillance of Jones, a suspected drug dealer,[109] by planting a GPS device on his vehicle and monitoring its publicly visible movements twenty-four hours per day for twenty-eight days without a valid warrant.[110] The district court, relying primarily on *Knotts*, held that the information gained from the movement of the car on public roads was admissible, but that any data gained from the car while it was parked in Jones's garage at home had to be suppressed.[111]

On appeal, the United States Court of Appeals for the District of Columbia Circuit disagreed, overturned Jones's conviction, and held that the warrantless tracking with the GPS device was a search within the meaning of the Fourth Amendment, even when it occurred

expectation of privacy."). *But see* People v. Weaver, 909 N.E.2d 1195, 1201-03 (N.Y. 2009) (holding that warrantless GPS surveillance violated the analogue to the Fourth Amendment in the New York Constitution).

[107] *See Jones*, 132 S. Ct. at 946 (documenting the events leading up to the prosecution and providing the procedural history of *Jones*).

[108] *See id.* (disagreeing with the previous holding of *Knotts* and subsequent similar cases).

[109] *See id.* at 948 (The police suspected Jones of cocaine trafficking). Their investigation included visual surveillance of Jones and the area around the nightclub that he owned, the installation of a fixed camera near the nightclub, a "pen register" that showed the telephone numbers of all calls to or from Jones's telephone, and a wiretap of Jones's cellular phone. Based on all of the information that they gained from tracking Jones's movements, the police obtained and executed a search warrant for Jones's stash house, which revealed a cache of drugs and money. After Jones was indicted, he moved to suppress the information gained from the GPS tracking device. The GPS logs were important at trial because they linked Jones to the stash house. *Id.* at 948-49. Jones had two trials. At the first, the jury acquitted him on multiple charges, but could not reach a verdict on the charge of conspiring to distribute cocaine and cocaine base, and the court declared a mistrial. *Id.* at 948. After the second trial, the jury found him guilty of the conspiracy charge, and the court sentenced him to life imprisonment. *Id.* at 949.

[110] *See id.* at 948 (demonstrating the police had obtained a warrant authorizing them to install and monitor the GPS device, but the warrant required that the device be installed within ten days of its issuance and only in the District of Columbia). The police attached the GPS device to the undercarriage of the car on the eleventh day while the car was parked in Maryland. For these reasons, the Government conceded that their placement of the device was not in compliance with the warrant. However, they argued that a warrant was not required. *Id.* at 948 n.1.

[111] *See id.* at 964 (illustrating the difference between how the Court treats a car in motion versus a car at rest).

on public roads.[112] The D.C. Circuit concluded that the district court had erred in failing to suppress all of the information that the police had obtained as a result of the GPS surveillance because it constituted precisely the type of "dragnet-type law enforcement practice[]" that the *Knotts* court had distinguished from the tracking beeper, reasoning:

> Here the police used the GPS device not to track Jones's "movements from one place to another," *Knotts*, 460 U.S. at 281, 103 S. Ct. 1081, but rather to track Jones's movements 24 hours a day for 28 days as he moved among scores of places, thereby discovering the totality and pattern of his movements from place to place to place.[113]

The circuit court concluded:

> First, unlike one's movements during a single journey, 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. Second, the whole of one's movements is not exposed *constructively* even though each individual movement is exposed, because that whole reveals more – sometimes a great deal more – than does the sum of its parts.[114]

On appeal to the Supreme Court, the Government argued that the fact that GPS made police tracking more "efficient" did not invade an additional expectation of privacy that the tracked individual would otherwise have had—in other words, that the technology did not make public something that had previously been private.[115] The

[112] *See id.* at 949 (holding that the surveillance was not allowed despite the car being on public roads); United States v. Maynard, 615 F.3d 544, 568 (D.C. Cir. 2010) (implying that the court erred in its decision to allow GPS surveillance as a law enforcement practice).
[113] *Maynard*, 615 F.3d at 558.
[114] *Id.*
[115] *See id.* (determining that "whether an expectation of privacy is reasonable depends in large part upon whether that expectation relates to information that has been 'exposed to the public'").

essence of the Government's argument was that, because the GPS device could track the location of vehicles only as they traveled on the public roadways—as law enforcement agents could do with their own eyes if there were enough of them and they could move fast enough—nothing of constitutional consequence had occurred.[116] There was no search.[117]

In *Jones*, a unanimous Supreme Court rejected the Government's arguments, breathing some new life into the Fourth Amendment.[118] The Court affirmed the decision of the D.C. Circuit, unanimously agreeing that the Government's installation of the GPS device and subsequent tracking of Jones's movements constituted a search, but for different reasons.[119] For the majority, the problem was a narrow one: that the police had physically invaded Jones's private property in order to plant the device "for the purpose of obtaining information."[120] In hinging its decision on the police's trespass and analogizing the placement of the device to the police entering Jones's home without invitation, the majority declined to decide whether the search would have violated the Fourth Amendment if the GPS tracking device had been placed on Jones's vehicle in a public parking lot – *i.e.*, whether the high-tech tracking itself was a search.[121]

For five concurring justices,[122] the issue was a broader one: the Government's warrantless access to and use of electronic metadata, including video surveillance in public places and business establishments, automatic toll-collection systems on highways (FastPass), devices that allow motorists to signal for roadside assistance (Onstar), location data from cell-phone towers, and records kept by online

[116] Transcript of Oral Argument at 60, *Jones*, 132 S. Ct. 945 (No. 10-1259) (concluding that there was no additional expectation of privacy).
[117] *See Jones*, 132 S. Ct. at 954 (holding there was no Fourth Amendment violation).
[118] *See id.* (affirming the Court of Appeals for the D.C. Circuit).
[119] *See id*. (addressing the various reasons for the conduct of a proper search using a GPS device).
[120] *Id.* at 949.
[121] *See id*. (distinguishing that the property occupied in this current case was private property).
[122] *See id*. at 954 (Sotomayor, J., concurring) (noting that although she joined the majority in its narrow property-rights holding, Justice Sotomayor made clear that she would have agreed with the four concurring justices finding that the GPS tracking was a search even if the placement of the device had not occurred on Jones's private property).

merchants.[123] During oral argument, several justices expressed concern that the ease with which the Government can now aggregate data could challenge long-held expectations of privacy.[124]

Justice Sotomayor, in a position with which this Article agrees, insisted that the act of using technology to aggregate large amounts of data, even if such data were already individually observable by the police in other form(s), could itself be an invasion of privacy of constitutional significance:

> [I]t may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. People disclose the phone numbers that they dial or text to their cellular providers; the URLs that they visit and the e-mail addresses with which they correspond to their Internet service providers; and the books, groceries and medications they purchase to online retailers. 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.[125]

---

[123] *See Jones*, 132 S. Ct. at 964 (Alito, J., concurring) (determining that new technologies make monitoring "relatively easy and cheap").

[124] *See* Transcript of Oral Argument at 10-11, *Jones*, 132 S. Ct. 945 (No. 10-1259). Justice Alito posed the following question: "But with computers, it's now so simple to amass an enormous amount of information about people that consists of things that could have been observed on the streets, information that was made available to the public…[I]sn't there a real change in this regard?" *Id.* at 11.

[125] *Jones*, 132 S. Ct. at 957 (Sotomayor, J., concurring). Justice Kagan took a similar position in her concurring opinion in *Jardines*:

> For me, a simple analogy clinches this case—and does so on privacy as well as property grounds. A stranger comes to the front door of your home carrying super-high-powered binoculars. He doesn't knock or say hello. Instead, he stands on the porch and uses the binoculars to peer through your windows, into your home's furthest corners. It doesn't take long (the binoculars are really very fine): In just a couple of minutes, his uncommon behavior allows him to learn details of your life you disclose to no one. Has your "visitor" trespassed on your property, exceeding the license you have granted to members of the public to, say, drop off the mail or distribute campaign flyers? Yes, he has. And has he also invaded your "reasonable expectation of privacy," by

While the overlapping opinions of the individual justices were divided on the rationale for the Court's holding, they collectively suggested that a majority of the Court is prepared to apply broad privacy principles to bring the Fourth Amendment's ban on unreasonable searches and seizures into the digital age, at a time when law-enforcement officials can gather voluminous amounts of personal information, in the absence of individualized suspicion, without ever physically intruding upon a protected area.[126]

C. Good News, You're Not Paranoid: Large-Scale Data Mining

The Obama Administration has recently proposed an end to the systematic collection of Americans' telecommunications metadata.[127] The proposal would not end all forms of data collection and mining, however, leaving in place bulk collection of data pertaining to international money transfers.[128] At the same time, the Obama administration has loosened the restrictions on how counterterrorism analysts may retrieve, store, and search the data gathered by government agencies other than the NSA "for purposes other than national security threats," making the search and storage of information held outside of the N.S.A. database about Americans easier.[129] New guidelines allow the NCTC to keep and analyze information gathered about American citizens and residents without suspected ties to terrorism for much longer.[130] The new guidelines will permit analysts

> nosing into intimacies you sensibly thought protected from disclosure? Yes, of course, he has done that too.

Jardines, 133 S. Ct. at 1418 (Kagan, J., concurring) (citations omitted).

[126] *See Jones*, 132 S. Ct. at 954 (discussing the Court's willingness to extend a broad interpretation of privacy principles with regard to the Fourth Amendment's ban on unreasonable searches and seizures).

[127] *See* Charlie Savage, *Obama to Call for End to N.S.A.'s Bulk Data Collection,* N.Y. TIMES (Mar. 25, 2014) [hereinafter C. Savage] *archived at* http://perma.cc/C67R-3H89 (highlighting a proposal that would end the N.S.A.'s systematic collection of data).

[128] *See id.* (noting that "the C.I.A., for example, has obtained orders for bulk collection of records about international money transfers handled by companies like Western Union").

[129] *See* Savage, *supra* note 23 (discussing that "the changes are intended to allow analysts to more quickly identify terrorist suspects").

[130] *See* Sari Horwitz & Ellen Nakashima, *New counterterrorism guidelines permit data on U.S. citizens to be held longer,* WASH. POST. (Mar. 22, 2012), *archived at*

to make more copies of entire databases, such as immigration databases, and data mine them using complex algorithms to search for patterns that could indicate a threat.[131] The new guidelines also relax the restrictions on how long these data may be stored, permitting the Government to retain such information for up to five years.[132]

These new data-mining policies come at the same time as legislation and court rulings are giving the Government greater access to telecommunications information.[133] The House of Representatives has twice passed the Cyber Intelligence Sharing and Protection Act ("CISPA"), which would establish an information-sharing scheme between the NSA and corporate networks for the ostensible purpose of promoting cyber security.[134] The proposed legislation would permit companies to get a wide range of "cyber-threat" intelligence from

http://perma.cc/8CH7-Q5UA (establishing that the NCTC was created in 2004 by the Intelligence Reform and Terrorism Prevention Act as a clearinghouse for information from the various intelligence agencies to help connect the dots among the massive amounts of information collected). The NCTC maintains access to approximately thirty databases across the Government. *See id.*

[131] *See* Savage, *supra* note 23 ("In 2009, *Wired Magazine* obtained a list of databases that the FBI, one of the agencies that share information with the NCTC, had acquired. It included nearly 200 million records transferred from private data brokers like Choice Point, 55,000 entries on customers of Wyndham hotels, and numerous other travel and commercial records.").

[132] *See* Savage, *supra* note 23 (explaining that cooperating government agencies already have the individual data involved, but they are required to dispose of them after a few months if they do not lead to an active investigation). The previous limit for storing this data had been 180 days, after which they had to be destroyed. The new regulations allow the NCTC to retain and mine these existing resources more thoroughly over a longer period of time. *See id.*

[133] *See* Savage, *supra* note 127 (discussing the increased availability of telecommunications information to the government).

[134] *See* Morgan Little, *CISPA legislation seen by many as SOPA 2.0*, L.A. TIMES (Apr. 09, 2012), *archived at* http://perma.cc/56RS-QQEN (declaring that the "goal of CISPA is to create new channels for communication between government intelligence entities and private firms regarding potential and emerging cyber-security threats"); *see also* Mathew J. Schwartz, *CISPA Cybersecurity Bill, Reborn: 6 Key Facts*, INFORMATION WEEK (Feb. 14, 2013), *archived at* http://perma.cc/CH7D-8FS4 (noting that the CISPA was reintroduced by the House Intelligence Committee); Hayley Tsukayama, *CISPA: Who's for it, who's against it and how it could affect you*, WASH. POST (Apr. 27, 2012), *archived at* http://perma.cc/9PZJ-HQ8P (stating that "CISPA could be interpreted to allow companies to share any of their customers' personal data as long as the companies say that the information is related to a 'cyber threat.' That includes agencies such as the Department of Homeland Security and the National Security Agency").

the Government and identify hackers by their electronic signatures and Internet addresses, but it could also create a reciprocal backdoor surveillance system through which the NSA could access the personal, private consumer data being held by the participating companies, with no consumer notice or court oversight.[135]

In addition, many police departments engage in cell-phone tracking to obtain the records and locations of cellular telephone users without probable cause.[136] It is increasingly common for the police to tail cell phones virtually, "using either the phone's own GPS or cellular triangulation," without a warrant or subpoena.[137] Other agencies have sought information about all of the cell-phone numbers that used a cell tower "at a particular location in a given period."[138] "Law enforcement tracking of cell phones, once the province mainly of federal agents, has become a powerful and widely used surveillance tool for local police officials, with hundreds of departments, large and small, often using it aggressively with little or no court oversight."[139]

The Supreme Court has not yet addressed the issue, but the United States Court of Appeals for the Third Circuit recently held that the Government did not need a search warrant to *subpoena* retrospective (*i.e.*, historical) cell-phone location information from telecommunications companies in order to track the travel of the phone's

---

[135] *See* Little, *supra* note 134 (noting that CISPA deals primarily with "cyber threat intelligence" which is defined as "information in the possession of an element of the intelligence community directly pertaining to a vulnerability of, or threat to, a system or a network of a government information, intellectual property, or personally identifiable information"); Schwartz, *supra* note 134 (classifying CISPA as a "controversial piece of cybersecurity legislation focused on information sharing"); Tsukayama, *supra* note 134 (quoting Facebook Vice President of Public Policy Joel Kaplan, "if the government learns the intrusion or other attack, the more it can share about that attack with private companies (and the faster it can share the information), the better the protection for users and our systems").

[136] *See* Michelle Maltais, *Police tracking of cellphones raises concerns,* L.A. TIMES (Apr. 4, 2012), *archived at* http://perma.cc/PZ8Y-8DD3 (describing the increasing trend of police departments using cell phone tracking to obtain information on users without obtaining a warrant).

[137] *See id.* (noting the increasing trend of police tracking the whereabouts of US citizens using the cell phone GPS of the user without a subpoena).

[138] *See id.*

[139] *See* Eric Lichtblau, *Police Are Using Phone Tracking as a Routine Tool,* N.Y. TIMES (Mar. 31, 2012), *archived at* http://perma.cc/2VH6-JLKQ ("While many departments require warrants to use phone tracking in nonemergencies, others claim broad discretion to get the records on their own.").

user.[140] Several state supreme courts have disagreed, holding that their state constitutions require probable cause and a search warrant to obtain such information.[141]

As the *New York Times* recently noted, "[t]he practice has become big business" for cellular telephone companies, "with a handful of carriers marketing a catalog of 'surveillance fees' to police departments to determine a suspect's location, trace phone calls and texts, or provide other services."[142] "[T]he wide use of cellular-telephone surveillance has seeped down to even small, rural police departments in investigations unrelated to national security," and some departments log dozens of traces a month for both emergencies and routine investigations.[143] "[P]olice departments have gotten wireless carriers to track cellular-telephone signals back to cell towers as part of nonemergency investigations to identify all the callers using a particular tower . . . ."[144] The ubiquitous nature of cellular phones has made them virtual biographers of daily life, a treasure trove of information about contacts and travels.[145] Carriers can "clone" cellular telephones and download text messages while they are turned off.[146] This wide use of cell tracking raises legal and constitutional questions, particularly when the police act without judicial

[140] *See In re* Application of U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to Gov't, 620 F.3d 304, 319 (3d Cir. 2010) (holding that if there are "specific and articulable facts showing that there are reasonable grounds to believe that" the contents of a wire or electronic communication, or the record or other information sought, are relevant, cell phone location information can be obtained).

[141] *See* State v. Earls, 70 A.3d 630, 646 (N.J. 2013) (holding that the New Jersey Constitution required the police ordinarily to get a search warrant before obtaining location information from Earls' cellular-telephone service provider, absent a recognized exception to the warrant requirement).

[142] *See* Lichtblau, *supra* note 139 (explaining that "cell carriers, staffed with special law enforcement liaison teams, charge police departments from a few hundred dollars for locating a phone to more than $2,200 for a full-scale wiretap of a suspect, records show").

[143] *See* Lichtblau, *supra* note 139 (noting that even some small "police departments [have] found cellular-telephone surveillance so valuable that they have acquired their own tracking equipment to avoid the time and expense of having the phone companies carry out the operations for them").

[144] Lichtblau, *supra* note 139.

[145] *See* Lichtblau, *supra* note 139 (describing cell phones as possessing the ability to record our daily activities in detail).

[146] *See* Lichtblau, *supra* note 139 (reporting that cell phone service providers have the ability to take a snap shot of a subscriber's cellular information).

orders.[147] There is a great deal of uncertainty over "what information" the police are entitled to obtain from cellular-telephone companies, "what standards of evidence they must meet, and when courts must get involved."[148]

Meanwhile, technology companies, academic institutions, and research divisions of the federal government are investing heavily in the hunt to acquire, analyze, and monetize Big Data.[149] Based on the premise that real-world (RW) characteristics are reflected in virtual-world (VW) behavior, the Reynard program of the Intelligence Advanced Research Projects Activity (IARPA),[150] which is a division of the Office of the Director of National Intelligence, has been sponsoring research that can identify behavioral indicators in VWs and massive multiplayer online games that are related to the RW characteristics of the users.[151] The attributes in which IARPA is interested include gender, age, economic status, educational level, occupation, ideology, "level of influence," geographic location, native language, and culture.[152]

The Department of Justice has funded research into the "automated detection and prevention of disorderly and criminal activities" as part of its Sensor Surveillance Program.[153] The goal of the program is to "develop methods for automatically detecting and preventing criminal and disorderly activities using an intelligent video system" in crowded places like public parks and schools.[154] The de-

[147] *See* Lichtblau, *supra* note 139 (suggesting that the use of cell tracking raises constitutional concerns).
[148] *See* Lichtblau, *supra* note 139 (contending there is still a lack of clarity over what information may be seized from a cell phone without a warrant).
[149] *See About IARPA*, INTELLIGENCE ADVANCED RES. PROJECTS ACTIVITY, *archived at* http://perma.cc/ZDU8-SXH8 (noting a specific example of an institution investing heavily into big data).
[150] *See id.* (explaining that the IARPA's mission is to sponsor research programs that have the potential to provide an intelligence advantage to the United States over future adversaries).
[151] *See Reynard*, INTELLIGENCE ADVANCED RES. PROJECTS ACTIVITY, *archived at* http://perma.cc/DK79-MENA/ (identifying behavioral indicators in virtual worlds that are related to real world characteristics of the users).
[152] *See id.* (listing the varied attributes that IARP collects).
[153] *See, e.g.*, NILS KRAHNSTOEVER, AUTOMATED DETECTION AND PREVENTION OF DISORDERLY AND CRIMINAL ACTIVITIES 1 (2011), *archived at* https://perma.cc/BGQ6-KGK6 (providing an unpublished report submitted to the Department of Justice).
[154] *Id*.

veloped technology goes "beyond simple motion-based behavior features and can estimate meaningful social relationships between people and groups."[155] The technology uses this information for "semantically high-level behavior and scenario recognition," including group formation and dispersion, agitation, "face detection and face recognition of non-cooperative individuals from a distance," and automatically estimating the social-network structures of groups from videos.[156] The program has led to the development of a "wide range of intelligent video capabilities" that will "allow law enforcement to gain insight into the ways that people behave and interact, as well as into the social structure behind their interactions."[157]

Last year, the National Science Foundation awarded $10 million to the A.M.P. Expedition, which stands for "algorithms machines people," at the University of California at Berkeley, a team of professors and graduate students who are sponsored by corporations like Google and Oracle to "take an interdisciplinary approach" to Big Data analysis.[158] Their goal is to "combine traditional database science with new techniques that harness the power of cloud and cluster computing to handle the massive scale" of the modern data landscape.[159]

More recently, the *New York Times* has reported that, since 2010, the NSA has been taking advantage of its huge collections of both domestic and international metadata, without individualized suspicion or a court order, to create "sophisticated graphs of some Americans' social connections," which can "identify their associates, their locations at certain times, their traveling companions, and other personal information."[160] The program was "intended to help the agency 'discover and track'" 'contact chains'" between "intelligence targets overseas and people in the United States."[161] The program authorized the agency to conduct "large-scale graph analysis on very large sets of communications metadata without having to check [the] foreignness" of every e-mail address, phone number, internet proto-

[155] *Id.*
[156] *Id.*
[157] *Id.* at 1-2.
[158] *See* Carstensen, *supra* note 11 (citing a 2012 statistic about A.M.P. funding).
[159] Carstensen, *supra* note 11.
[160] James Risen & Laura Poitras, *N.S.A. Gathers Data on Social Connections of U.S. Citizens*, N.Y. TIMES, at A1 (Sept. 29, 2013) [hereinafter Risen & Poitras, *Social Connections*], *archived at* http://perma.cc/5GWP-NDHE.
[161] *Id.*

col (IP) address, or other identifier.[162] "The agency can augment the communications data with material from public, commercial, and other sources, including bank codes" for domestic and foreign transactions, insurance information, information from online social networks like Facebook profiles, passenger manifests, voter registration rolls, location information from services like GPS and TomTom, property records, tax data, and billing records, without restrictions on subsequent use.[163] "Vast amounts" of this data "flow daily from the agency's fiber-optic cables, corporate partners, and foreign computer networks that have been hacked," including 1.1 billion cellular-telephone records per day.[164] "[T]he NSA correlates 164 'relationship types' to build social networks and what the agency calls 'community of interest' profiles, using queries like 'travelsWith, hasFather, sentForumMessage, employs.'"[165] NSA analysts can use that information to "develop a portrait of an individual," one that may be "more complete and predictive of behavior than could be obtained by listening to phone conversations or reading e-mails."[166]

There is reason to believe that Americans would object to warrantless data mining—would harbor and expect the courts to protect an expectation of privacy in their aggregate personal information—if only they were aware of its scope.[167] A recent, nationwide survey of cellular-telephone users, for example, found that eighty percent of them objected to their phones transferring their phone numbers to a store at which they had purchased something and ninety-six percent would not be willing to have their information shared with a store whose site they simply visited.[168] Under *Katz*,

---

[162] *Id.*

[163] *See id.* (detailing the breadth of the sources that the NSA can augment without indicated restrictions).

[164] *See id.* (describing the flow of data from hacked networks). The NSA also requested funds from Congress in 2013 to develop a metadata repository that would be capable of recording 20 billion "record events" each day. The recordings are available to analysts within sixty minutes. The NSA processes the data automatically in order to make later queries run more quickly and to identify new surveillance targets.

[165] *Id.*

[166] Risen & Poitras, *Social Connections*, *supra* note 160.

[167] *See* Sengupta, *Pay Phone*, *supra* note 12 (suggesting that Americans are uneasy with the idea that their phones divulge personal information).

[168] *See* Sengupta, *Pay Phone*, *supra* note 12(discussing consumers' unwillingness to share their phone numbers with public businesses).

courts should recognize the normative reasonableness of these expectations.[169]

D. At Long Last: The Unified Theory

The Supreme Court has refused to recognize a reasonable expectation of privacy in the numbers dialed from or to a telephone, reasoning that, by voluntarily conveying numerical information to the telephone company, a customer has forfeited any reasonable expectation of privacy in the numbers dialed.[170] In *Smith v. Maryland*, the Court drew a clear distinction between the numbers dialed and the contents of the calls (the monitoring of which would require a warrant and probable cause) – the precursor to the metadata/contents distinction drawn by the Government in data-mining cases today.[171]

Of course, *Smith*'s distinction between the numbers dialed (*i.e.*, metadata) and the contents of the conversations is the problem.[172] In defending the NSA's warrantless data mining, the Government relies on *Smith*, arguing: "Supreme Court precedent makes clear that participants in telephone calls lack any reasonable expectation of privacy under the Fourth Amendment in the metadata records

---

[169] *See Katz*, 389 U.S. at 361 (explaining expectations of privacy that society has deemed reasonable).

[170] *See Smith*, 442 U.S. at 742 (doubting that people in general have a reasonable expectation of privacy since they must convey the telephone number dialed to the telephone company when placing a call).

[171] *See Smith*, 442 U.S. at 740-42 (distinguishing from *Katz* since the pen register was installed at the telephone company, and did not reveal any information other than the number dialed). State supreme courts have disagreed with the Court's analysis and required warrants and probable cause under their state constitutions. *See, e.g.*, State v. Thompson, 760 P.2d 1162, 1165, 1167 (Idaho 1988) (holding that defendant had a reasonable expectation of privacy under the Idaho state constitution in a record showing telephone numbers to which defendant made calls, and finding the dissent in *Smith* persuasive).

[172] *See* Risen & Poitras, *Social Connections*, *supra* note 160 (noting that *Smith* is the legal underpinning of the NSA's new surveillance programs).

> The legal underpinning of the policy change… was a 1979 Supreme Court ruling that Americans could have no expectation of privacy about what numbers they had called. Based on that ruling, the Justice Department and the Pentagon decided that it was permissible to create contact chains using Americans' 'metadata,' which includes the timing, location and other details of calls and e-mails, but not their content.

Id.

generated by their telephone calls and held by telecommunications service providers."[173]

The *Smith* metadata/contents distinction is an outdated one, which has been undercut by the Court's more recent jurisprudence in cases like *Kyllo, Jones,* and *Jardines*.[174] Data mining enables investigators and corporations to detect (and make "public") new information that was previously private: patterns of behavior.[175] For example, law-enforcement agents can compile a list of an individual's associates, determine an individual's location history, "acquire clues to religious or political affiliations, and pick up sensitive information like regular calls to a psychiatrist's office, prescription-refill information from a local pharmacy, late-night messages to an extramarital partner, or exchanges with a fellow plotter from phone and e-mail metadata."[176] There is a meaningful distinction between gathering individual pieces of raw data and combing large databases to find complex patterns in their collective metadata, and Fourth Amendment jurisprudence should recognize it.[177]

One distinction that unifies the areas in which the Court has indicated a willingness to find that a form of government surveillance constitutes a search (*e.g.*, electronic eavesdropping, wiretapping, and thermal imaging) while distinguishing them from the areas in which it has not (*e.g.*, aerial surveillance or garbage collection) is the theme of technological advancement.[178]

---

[173] *See* WHITE PAPER, *supra* note 25, at 19 (stating how the telephony metadata collection program is permissible under the Fourth Amendment).

[174] *See Kyllo*, 533 U.S. at 33 (noting that technologically enhanced perception may be a violation of a reasonable expectation of privacy); *Jones*, 132 S.Ct. at 954 (questioning how long a suspect can be observed before violating their reasonable expectation of privacy); *see also Jardines*, 133 S.Ct. at 1417-18 (holding that the use of a police canine to detect the presence of narcotics from the porch of a residence was an invasion of the curtilage of the home and a search under the Fourth Amendment).

[175] *See Data Mining, Dog Sniffs, and the Fourth Amendment*, *supra* note 36, at 691 (presuming that with the use of data mining, information which was once private will be more likely to become public).

[176] Risen & Poitras, *Social Connections*, *supra* note 160.

[177] *See* Risen & Poitras, *Social Connections*, *supra* note 160 (observing the patterns which form between various metadata sources).

[178] *See* Transcript of Oral Argument at 10-11, *Jones*, 132 S.Ct. 945 (No. 10-1259) (offering an explanation for how technological advancements have changed the way courts look at surveillance).

1. Automation

Data mining often does not involve or require actual knowledge, by a human being, of the material being "searched."[179] Unlike the pay-phone conversations that live agents listened to (with electronic enhancement) in *Katz*, the collection of the individual data points composing the Government's databases is automated.[180] For example, unlike human surveillance or even the beeper at issue in *Knotts*, the type of GPS surveillance at issue in *Jones* does not require human participation or monitoring, at least in real time, making it possible for a police agency to track, collect, store, and later recall data on an almost infinite number of people using automated GPS tracking.[181] Computers also analyze the sum of that data automatically, using complex algorithms.[182] No human being reads through the metadata looking for patterns; it would be impossible for a human being to do so.[183] Computational linguistics, or Natural Language Processing (NLP), software would even allow the Government to "search" the contents of telephone, text, instant messaging, and e-mail conversations (think the fabled NSA computers that for decades have reportedly "listened" to Americans' phone conversations searching for those with words like "kill" and "President" in proximity), without any live person seeing, hearing, reading those conversations.[184]

---

[179] *See id*. (highlighting many methods of searching for information without the knowledge of the person being searched).

[180] *See Katz*, 88 S.Ct. at 369 (observing the old fashion method of using payphones as government surveillance).

[181] *See Jones*, 132 S.Ct. at 948 (providing an example of monitoring without direct human participation).

[182] *See* Transcript of Oral Argument at 11, *Jones*, 132 S.Ct. 945 (No. 10-1259) (commenting on the ease at which information is collected, stored and retrieved with the addition of computers).

[183] *See id.* at 13 (implying that a computer is significantly more efficient at surveillance than any human could be).

[184] *See, e.g.*, David M. Bei et al., *Latent Dirichlet Allocation*, 3 J. MACHINE LEARNING RESEARCH 993 (2003) (describing the latent Dirichlet allocation model for the automated collection of discrete linguistic data, such as text corporations); ALEXANDER CLARK ET AL., THE HANDBOOK OF COMPUTATIONAL LINGUISTICS AND NATURAL LANGUAGE PROCESSING (Alexander Clark et al. eds., 2010) (providing an overview of the concepts, methodologies, and applications of computational linguistics and NLP); DANIEL JURAFSKY & JAMES H. MARTIN, SPEECH & LANGUAGE PROCESSING (2000) (describing web-based language technologies); CHRISTOPHER D. MANNING & HINRICH SCHUTZE, FOUNDATIONS OF STATISTICAL NATURAL

The Government has defended the NSA's Prism program in part on this ground, noting: "critically, although a large amount of metadata is consolidated and preserved by the Government, the vast majority of that information is never seen by any person."[185] Google has also recently advanced this distinction – between live surveillance and automated monitoring – in response to a newly filed class-action lawsuit claiming that it engaged in illegal wiretapping when it "applie[d] automated (non-human) scanning to e-mails involving Gmail users."[186] As part of its e-mail processing, "Google's automated systems scan e-mail content" to filter out spam, detect computer viruses, render e-mail messages word searchable, and "automatically sort incoming e-mail."[187] The litigation has revealed that "[t] systems are also used to display advertisements targeted to e-mail content."[188] In its recent motion to dismiss, Google has claimed, because the processes at issue (scanning e-mails in order to transmit and data mine them) are "completely automated and involve no human review," they do not constitute electronic surveillance.[189]

Automation, however, does not and should not end the search inquiry If anything, the automated nature of modern data mining makes it more, not less, intrusive.[190] Furthermore, all of the points of data that are being mined automatically remain within the construc-

---

LANGUAGE PROCESSING (1999) (describing statistical NLP); THOMAS MCENERY, CORPUS LINGUISTICS: AN INTRODUCTION 114 (1996) (describing the use of corpora in discourse analysis).

[185] *See* WHITE PAPER, *supra* note 25, at 4.

[186] *See* David Gilbert, *Google To Gmail Users—You Should Never Have Expected Email Privacy,* IBT *archived at* http://perma.cc/5YSU-66QD ; Defendant Google's Inc.'s Objections to Plaintiffs' Reply Evidence in Support Of Consolidated Motion For Class Certification, *In re:* Google Inc. Gmail Litigation, 2013 WL 7394856 at 2 (N.D. Cal. Dec. 26, 2013) (No. 5:13-md-021430-LHK (PSG)) [hereinafter Google's Objection to Class Certification]; *In re:* Google Inc. Gmail Litigation, No. 13-MD-02430-LHK, 2013 WL 5423918 (N.D. Cal. June 13, 2013) (introducing the issues concerning the use of automated surveillance on Gmail users).

[187] *See* Google's Objection to Class Certification , *In re Google,* 2013 WL 7394856, at 3.

[188] *Id.* at 3.

[189] *Id.* at 2-4.

[190] *See* Savage, *supra* note 23 (demonstrating the vast database of records the government holds).

tive possession of the Government, and presumably it has at least implied knowledge of all of those individual points.[191]

2. Aggregation

The police have always been able to surveil *anyone* and collect evidence that they have abandoned or left in plain view.[192] If that evidence added to rather than dissipated their suspicions, the investigation would eventually ripen into a prosecution.[193] Because of resource constraints, however, they would only surveil people against whom they had some individualized suspicion in the first instance – people who were already suspects.[194] The police of the past were never able to surveil *everyone*.[195] But today, they both can and do surveil people prior to suspicion as a way of looking for suspects.[196]

Traditionally, searches have had the following chronology: suspect → surveillance.[197] Increasingly, the chronology has become surveillance → suspect.[198]

---

[191] *See* Savage, *supra* note 23 (implying that intelligence officials' failure to "connect the dots" before the "underwear bomber" attempted to bomb an airliner shows they had presumptive knowledge based on the data they collected).
[192] *See Katz*, 389 U.S. at 361 (Harlan, J. concurring) (affirming that the police are allowed to search within plain view).
[193] *See id.* at 353 (observing the differences between what constitutes a search that allows for prosecution and that do not).
[194] *See id.* at 354 (demonstrating an instance in which resource constraints affected both the scope and duration of the police's telephone electronic surveillance).
[195] *See id.* at 357 (requiring probable cause and warrants for lawful police surveillance).
[196] *See id.* at 355 (determining that "under sufficiently 'precise and discriminate circumstances,' a federal court may empower government agents to employ a concealed electronic device 'for the narrow and particularized purpose of ascertaining the truth of the allegations' of a 'detailed factual affidavit alleging the commission of a specific criminal offense'"(quoting Osborn v. United States, 385 U.S. 323, 329-30 (1966))).
[197] *See* Bruce Schneier, *Metadata Surveillance*, IEEE SECURITY & PRIVACY (2014), *archived at* http://perma.cc/R47C-JXWK (describing that developing technologies has made it possible for police to "tail everyone").
[198] *See id.* (concluding that because of developing technologies, police can now perform analyses that otherwise were not possible).

Here is a thought experiment to illustrate this point. You and three friends each purchase three disposable cell phones using your credit cards. Every Tuesday, you place one phone call from 12:00 – 12:05 on your disposable phone to that of Friend #1 and one phone call from 12:05 – 12:10 to Friend #2. You rent a motel room for one month using your credit card. Friend #1 purchases electronics equipment at Radio Shack using her credit card. Friend #2 purchases diesel fuel using his. You purchase tropical fertilizer using yours. Friend #1 takes flying lessons. Friend #2 visits jihadist websites from his home computer. You use the words "Allah akbar," "al-Aqsa," and "drone" in your weekly phone calls. You Google "airport explosives detection" from your home computer. Each of you purchases a single one-way ticket on a flight from Portland, Maine (where none of you live) to Reagan National Airport in Washington, D.C. The list could continue, but you get the picture. What is the likelihood that your rented motel room is searched using a "sneak-peek" warrant, your financial records are secretly subpoenaed under the Patriot Act? The question, of course, is not really whether you would be searched, only when, where, how, by whom, and pursuant to what authority.

In *Jones*, the Government argued that characterizing data aggregation and mining from sources of information in which there is no reasonable expectation of privacy as searches for Fourth Amendment purposes would in effect constitutionalize inefficiency and inconvenience, forcing the police to collect evidence in the grueling, haphazard, old-fashioned way, when they could instead conduct a modern and efficient search with an algorithm and a few clicks of a mouse.[199] In its defense of the NSA data-mining program, the Government dismissed, with little analysis, the suggestion that "the volume of records" whose metadata were being collected and analyzed "convert[ed] that activity into a search."[200] Once the amount of data is so great and the analysis of it is so complex that neither could be accomplished at the human scale, however, the mining and analysis should no longer be subject to the antiquated Fourth Amendment rules that were developed with human investigators, or even rudimen-

[199] *See Jones*, 132 S.Ct. at 950 (explaining that the wiretap used to gather information did not constitute an invasion of privacy).
[200] WHITE PAPER, *supra* note 25, at 20.

tary digital technology, in mind – *Smith*'s "numbers dialed" / "words spoken" dichotomy.[201]

The difference between data mining and old-fashioned surveillance, however, is not just in the volume of surveillance that can be performed or the amount of information gathered, but also the percentage of surveilled information that is innocent and the consequences of targeting that does not result in either exoneration or prosecution.[202] Because data mining involves combing through information belonging to people about whom the police have no suspicion, in the hope of developing suspicion against one or more of them, it results in people who would have essentially no likelihood of ever being "tailed" or eavesdropped being monitored without at least the protection of a "moment of truth" in which the Government either charges them or leaves them in privacy.[203] It has become the ultimate dragnet, and we are now all the usual suspects.[204] The State of California recognized the distinction between human monitoring of individual suspects and computer monitoring of a large population in its argument before the Court in *Ciraolo*.[205] It conceded that aerial surveillance of a house's curtilage could become unconstitutionally "invasive" if more advanced technology were developed that could reveal "those intimate associations, objects or activities otherwise imperceptible to police or fellow citizens."[206]

The Court had two prime opportunities to extend the reasoning in cases like *Katz* and *Kyllo* to searches involving other types of high-tech surveillance in *Jones* (GPS tracking) and *Jardines* (dog sniffs) and create a unified theory of when enhanced surveillance becomes a "search" for Fourth Amendment purposes, but it declined to do so (or, for that matter, to reject this vision), deciding both cases in-

[201] *See* Smith, *supra* note 33 (specifying agencies that were given broad ability to conduct surveillance without a warrant post 9/11 through the Patriot Act, resulting in many innocent Americans being affected).
[202] *See* Smith, *supra* note 33 (cautioning "that means you're going to end up holding a lot of data about ordinary people who have nothing to do with your threat").
[203] *See Ciraolo*, 476 U.S. at 224 (comparing data mining to the aerial surveillance at issue and determining that both provide reasonable expectation of privacy).
[204] *See id.* at 226 (stating that "the essence of a Fourth Amendment violation is 'not the breaking of [a person's] doors, and the rummaging of his drawers,' but rather is 'the invasion of his indefeasible right of personal security, personal liberty and private property'").
[205] *See id.* at 218 (differentiating between whether police have physically invaded a constitutionally protected area and surveillance techniques through technology).
[206] *Id.* at n.3.

stead on narrower, technical trespass grounds.[207] This Article picks up where *Kyllo* left off, essentially proposing that Moore's Law should create a limiting principle under the Fourth Amendment.[208] Information technology will continue to grow exponentially, but the Fourth Amendment should be interpreted to permit the Government's ability to invade our privacy to grow only as human ability does.[209] In other words: a search has occurred at the point at which a mortal human being could no longer perform it.[210] This is, in a way, the rule that the Court suggested in *Kyllo* and that Justice Kagan proposed in *Jardines*.[211] All that it needs to do now is extend it explicitly beyond sensory enhancement to include the massive, high-speed data analysis performed across an entire population by complicated computer algorithms.[212]

3. Shelf Life

Much of the invasiveness of the scope, duration, and permanency of modern data collection and storage, however, comes after the search.[213] The data that are collected during this suspicionless

[207] *See Jones*, 132 S.Ct. at 949 (holding that a warrant is required to place a GPS tracking device on a car); *see also Jardines*, 133 S.Ct. at 1417 (requiring a warrant for a drug sniffing dog to intrude upon the curtilage of a home).
[208] *See Kyllo*, 533 U.S. at 34 (addressing that technological advancements limits the Fourth Amendment right to privacy).
[209] *See* Smith, *supra* note 33 (explaining the current coverage of the Fourth Amendment).
[210] *See Kyllo*, 533 U.S. at 33-34 (discussing how the advancement of technology has affected the definition of a search).
[211] *See id.* at 34 (inferring that the use of technology during a search should be limited to that of human capability); *Jardines*, 133 S.Ct. at 1418 (Kagan, J., concurring) (discussing how "drug-detection dogs are highly trained tools of law enforcement, geared to respond in distinctive ways to specific scents so as to convey clear and reliable information to their human partners. . . . Like [high-powered] binoculars, a drug-detection dog is a specialized device for discovering objects not in plain view (or plain smell)").
[212] *See* Transcript of Oral Argument at 11-12, *Jones*, 132 S. Ct. 945 (No. 10-1259) (noting that "it is possible to envision broader advances in technology that would allow more public information to be amassed and put into computer systems . . . [and] the remedy [for that] is through legislation").
[213] *See* Risen & Poitras, *Social Connections*, *supra* note 160 (detailing the NSA's ability to retain and review collected data indefinitely after collection).

monitoring can be stored and searched indefinitely.[214] For example, if the NSA does not "immediately use" the phone and e-mail metadata that it collects daily on Americans, it can store them "for later use, at least under certain circumstances."[215]

Prior to the collection, storage, and data mining of personal digital data, if a search revealed no evidence against a suspect, the suspect's file was eventually closed.[216] Today, if the metadata search did not reveal sufficient evidence of criminal activity, the suspect still might end up residing permanently in Caimanera because that is the new consequence of the Government suspecting without sufficient evidence to prove.[217]

President Obama has recently seemed to acknowledge the independent invasion of privacy that this long-term storage and search potential creates, as the *Times* reported, when he proposed requiring the NSA to deleted data that it collects abroad "after a certain period of time" and "limiting its use to specific security requirements, like counterterrorism and cybersecurity."[218] These proposed time and scope limitations, however, would apply to foreign data collection, not the mining of domestic metadata.[219]

IV. CONCLUSION

The inescapable question that arises from these realities is: what, if any, are the constitutional limits of Government watchfulness over our daily lives collectively when it lacks any suspicion to monitor each of us individually? Returning to the thought experiment about the fake terrorist cell, most Americans might want the police to search that hotel room, even without judicial authorization or proba-

[214] *See* Risen & Poitras, *Social Connections*, *supra* note 160 (explaining that the NSA is capable of storing collected data for future review).
[215] *See* Risen & Poitras, *Social Connections*, *supra* note 160 (acknowledging that the NSA stores data that it collects).
[216] *See* Landler & Savage, *supra* note 5 (noting "that data collected abroad be deleted after a certain period and limiting its use to specific security requirements, like counterterrorism and cybersecurity").
[217] *See* Landler & Savage, *supra* note 5 (defending the need for internet surveillance).
[218] *See* Landler & Savage, *supra* note 5 (acknowledging President Obama's stance on the potential importance of internet surveillance).
[219] *See* Landler & Savage, *supra* note 5 (discussing restrictions on foreign data collection and retention only).

ble cause. As Justice Alito blithely noted in his concurrence in *Jones*: "New technology may provide increased convenience or security at the expense of privacy, and many people may find the tradeoff worthwhile. And even if the public does not welcome the diminution of privacy that new technology entails, they may eventually reconcile themselves to this development as inevitable."[220]

Because this is an experiment and not a real plot, the search would reveal no explosives, and the flight from Maine to D.C. would be an uneventful one. But you would never again make a phone call that was not wiretapped, hold a job that required a security clearance, or fly on a commercial aircraft, because these are the collateral consequences of being a "suspect" in a world in which suspects are no longer ever "cleared," and you will never be notified or given an opportunity to challenge your new classification. Your data would also likely never be "expunged" from Government computers, but rather would be stored for possible later use.

The canon of constitutional avoidance notwithstanding,[221] the time has come for the Supreme Court to interpret the Fourth Amendment to stop the otherwise inexorable march of technology into every last corner of our personal lives. If surveillance is too inconvenient to be done by human beings, it is more, not less, of a search.

[220] *See Jones*, 132 S.Ct. at 962 (Alito, J., concurring).
[221] *See, e.g.,* INS v. St. Cyr, 533 U.S. 289, 299-300 (2001) (holding that "if an otherwise acceptable construction would raise serious constitutional problems and an alternative interpretation is fairly possible, the statute must be construed to avoid such problems").