Washington and Lee Law Review

Volume 72 | Issue 3 Article 13

Summer 6-1-2015

I Spy: The New Self-Cybersurveillance and the "Internet of Things"

Steven I. Friedland
Elon School of Law

Follow this and additional works at: https://scholarlycommons.law.wlu.edu/wlulr

 Part of the Fourth Amendment Commons, and the Privacy Law Commons

Recommended Citation
Steven I. Friedland, *I Spy: The New Self-Cybersurveillance and the "Internet of Things"*, 72 Wash. & Lee L. Rev. 1459 (2015), https://scholarlycommons.law.wlu.edu/wlulr/vol72/iss3/13

This Article is brought to you for free and open access by the Washington and Lee Law Review at Washington & Lee University School of Law Scholarly Commons. It has been accepted for inclusion in Washington and Lee Law Review by an authorized editor of Washington & Lee University School of Law Scholarly Commons. For more information, please contact lawref@wlu.edu.

I Spy: The New Self-Cybersurveillance

Steven I. Friedland*

> "It won't be a question anymore of whether things are connected. We're going to move toward a learning model where your home actually observes how you're living inside it and adapts itself toward your needs." George Yianni[1]

Abstract

Prior to the digital age, surveillance generally meant a government agent or private investigator engaged in a stakeout or observation detail that involved physical work, expense, and time. The digital age changed surveillance fundamentally. Today, we not only generate mountains of data for others, we also effectively surveil ourselves through digitally-connected, multifunctional smart devices, collectively described as the "Internet of Things."

Cybersurveillance accessed by the government, even when started as self-surveillance, raises complex and uncertain legal issues, especially when related to the Constitution. In United States v. Kyllo*, the Supreme Court was reticent to allow government agents to use technology that went through the walls of homes, spying on people within without a warrant under the Fourth Amendment. Current technologies allow the police to do that and more, especially when all of the data is pieced together and analyzed in a personal mosaic. The implications are profound. Is there anything left of the public/private distinction? Does the invisibility of data transfer undermine the separation of powers and the ability to effectively check and balance the Executive branch's spying operations? This paper examines the constitutional implications of the Internet of Things, arguing that unless models*

* The author wishes to thank the Elon School of Law librarian Lisa Watson for her terrific research assistance, as well as his research assistants, Kelly Holder, Ragan Riddle, Talia Nowicki, and Paige Vankooten, for their diligent and highly competent work.

1. Yianni invented the Philips Hue Connected Light Bulb.

of consent and privacy are changed, outdated legal rules will fail to protect the individual from the state in fundamental ways.

Table of Contents

I. Introduction

A quotidian routine likely occurs in millions of residences around the globe every morning. An adult stumbles out of bed in the pre-dawn winter, turns on the lights, grabs a cup of coffee, and operates the television remote to catch the news and traffic. She then adjusts the thermostat, checks her watch, and goes outside to start warming up her car. Several minutes later, she drives away.

The entire routine depicted above is now undergoing a profound transformation. The objects used in such activities now have multifunctional capabilities. While appealing to users for their convenience, the devices will generate personal, even intimate, information.[2] The so-called "Internet of Things" describes the way these devices can connect to each other through the Internet to generate and share information.[3] More than that, these devices can "learn" how to improve the functionality of their actions.[4]

The nature and journey of the information generated by "smart" home devices and wearable technology have considerable legal significance.[5] While the homeowner initially controls all of the devices, the information generated may be accumulated by the manufacturer that created the device and transferred to the commercial marketplace or, ultimately, the government.[6]

---

2. *See infra* Part II.B (describing how people use smart devices to monitor themselves).

3. *See* Sharon O'Malley, '*Internet of Things' Front and Center at Annual Consumer Electronics Show*, CONSTRUCTION DIVE (Jan. 15, 2015), http://www.constructiondive.com/news/internet-of-things-front-and-center-at-annual-consumer-electronics-show/353352/ (last visited June 12, 2015) (explaining that "techies call the smart home of the future 'the Internet of Things,'" which can be controlled by the homeowner using a smartphone application) (on file with the Washington and Lee Law Review).

4. *See id.* (describing a lighting device that knows to turn on bright lights when the family wakes up in the morning and dim lights before the family's normal wake-up time).

5. *See infra* Part II.B (contending that the amount of data collected by smart technology creates unprecedented opportunities for surveillance).

6. *See infra* Part II.A.2 (discussing the government's use of private companies to gather data about Americans).

The nature and quantity of information produced by devices whose form and function are separated will be extensive. The lighting device can "learn" the "household's daily patterns over time and set itself to turn on the lights just before the family starts arriving home in the evening."[7] The lighting mechanism can even learn to turn on low light when the occupant gets out of bed at night.[8] The television can be triggered by voice activation, which means it can "listen" to the speaker and anyone else talking in the room in which the set is located.[9] The smart thermostat can recognize whether anyone is in the house, how long occupants slept the night before, and which rooms are likely occupied, automatically lowering the thermostat in unoccupied areas to save energy.[10] The thermostat "learns" about the inhabitants and their propensities at home.[11] The watch provides the time, but can monitor the wearer—determining how many steps the person is taking in a day to show levels of activity, how well the wearer slept the night before, and even how the heart, a vital organ, is beating.[12]

The car in the above scenario has changed as well. It now can be started remotely, providing more time indoors for the driver,

---

7. O'Malley, *supra* note 3.

8. *Id.*

9. *See, e.g.*, *Not in Front of the Telly: Warning Over 'Listening' TV*, BBC (Feb. 9, 2015, 6:20 PM), http://www.bbc.com/news/technology-31296188 (last visited June 16, 2015) (on file with the Washington and Lee Law Review). The policy for the TV set "explains that the TV will be listening to people in the same room to try to spot when commands or queries are issued via the remote." *Id.* It further provides: "If your spoken words include personal or other sensitive information, that information will be among the data captured and transmitted to a third party." *Id.* (citation omitted).

10. *See* Kashmir Hill, *When Smart Homes Get Hacked: I Haunted a Complete Stranger's House Via the Internet*, FORBES (July 26, 2013, 9:15 AM), http://www.forbes.com/sites/kashmirhill/2014/11/07/how-did-law-enforcement-break-tor/ (last visited June 16, 2015) (describing a thermostat that monitors inhabitants' activity, learns their schedules and temperature preferences, and heats or cools the house as it deems appropriate) (on file with the Washington and Lee Law Review).

11. *Nest Thermostats*, NEST, https://nest.com/ie/thermostat/meet-nest-thermostat/ (last visited June 16, 2015) (describing the features of a smart thermostat) (on file with the Washington and Lee Law Review).

12. *See, e.g.*, *Fitbit*, FITBIT, http://www.fitbit.com/#i.1r2ovyecs6fal1 (last visited June 16, 2015) (on file with the Washington and Lee Law Review). The Fitbit can be placed on one's belt or around one's wrist. *Id.* In addition to keeping time, it can mark steps, sleep time and restfulness, heartbeats, and more. *Id.* It can be linked to the Internet to store this information. *Id.*

but also adding to the accumulated data points about the car's driving history[13]—from "where drivers have been, like physical location recorded at regular intervals, [to] the last location they were parked, distances and times traveled, and previous destinations entered into navigation systems."[14] Soon, vehicle-to-vehicle communication will occur when cars begin exchanging information.[15]

The owner's mobile phone is also a multifunctional device. It is only partly a phone, and is more accurately described as a portable computer. Even when the phone is not in use by the possessor, the location of the phone in relation to the nearest cell phone towers provide regular tracking,[16] becoming GPS locators as well.[17]

---

13. This information is shared with the manufacturer and third parties. Aaron M. Kessler, *Report Sees Weak Security In Cars' Wireless Systems*, N.Y. TIMES, Feb. 9, 2015, at B4.

14. *Id.*

15. *See id.* (noting vehicle-to-vehicle communication is expected to be available in the near future). While industry trade groups pushed to limit data collected for legitimate business purposes, a report by Senator Edward J. Markey, Democrat from Massachusetts, "says the phrase 'legitimate business purposes' is vague enough to allow for all kinds of collection, and asserts that clear federal rules should be established for what are permissible and appropriate uses of drivers' data." *Id.*

16. *See* Timothy Menard & Jeff Miller, *GPS Capabilities of the iPhone 4 and iPhone 3G for Vehicle Tracking Using FreeSim Mobile*, ACADEMIA, http://www.academia.edu/545842/Comparing_the_GPS_Capabilities_of_the_iPhone_4_and_iPhone_3GS_for_Vehicle_Tracking_using_FreeSim_Mobile (last visited June 16, 2015) (discussing how cell phone towers are used to identify the location of a phone) (on file with the Washington and Lee Law Reivew). The general location of cell phones is sometimes checked every seven seconds to determine what is the closest, and therefore the best, cell phone tower to use for signals. Steven M. Harkins, Note, *CSLI Disclosure: Why Probable Cause Is Necessary to Protect What Is Left of the Fourth Amendment*, 68 WASH. & LEE L. REV. 1875, 1877 (2011). Thus, mountains of data are not simply created, but also are gathered, stored, and analyzed to adapt to the persons and places being monitored.

17. *See* Laura M. Holson, *Privacy Lost: These Phones Can Find You*, N.Y. TIMES (Oct. 23, 2007), http://www.nytimes.com/2007/10/23/technology/23mobile.html?_r=0 (last visited June 16, 2015) (showing that, even at its inception, GPS technology began to limit personal privacy) (on file with the Washington and Lee Law Review); *see also* Darlene Storm, *Think You've Deleted Your Dirty Little Secrets? Before You Sell Your Android Smartphone . . .*, COMPUTERWORLD (July 9, 2014, 1:30 PM), http://www.computerworld.com/article/76496/data-privacy/think-you-deleted-your-dirty-little-secrets--before-you-sell-your-android-smartphone.html (last visited June 16, 2015) (showing the

If our homes and devices such as cell phones are able to spy on us—and even show what is occurring inside of our bodies—we are essentially creating new mass surveillance systems through self-cybersurveillance. The self-generated systems complement other forms of cybersurveillance being developed today over the Internet, on land, in the skies, and even in the seas.

The treasure trove of information produced by the self-surveillance systems would be a gold mine in any era. The sharing of this data can be especially pernicious. The data trail often is invisible; unlike a police tail or even drones overhead, the surveillance from the interconnected devices hums along silently, like an odorless gas. The devices raise no fear because the potential harms from shared information[18] are unseen and often far downstream.[19] The degradation of the private sphere thus is subtle but substantial.

Government acquisition of the data for use when and how it sees fit creates the most potential for harm as well as concomitant legal issues. While access by private parties can be very troublesome,[20] the government has police powers and can impose

---

massive amount of data that can be found on smartphones) (on file with the Washington and Lee Law Review).

18. Most manufacturers will be able to share user information. *See What Promises Are Being Made About Sharing Data with Third Parties?*, THE COMMON DATA PROJECT, http://commondataproject.org/paper-policies-thirdparties (last visited June 16, 2015) (listing common reasons that privacy policies provide for sharing data with third parties) (on file with the Washington and Lee Law Review).

19. Compare these interconnected devices with unmanned aerial devices or drones. The drones can often be seen and heard, providing the experience of intrusion. Drones, without a pilot, are perhaps even more intrusive because you can see them but not their "pilot." These drones are operated commercially and privately and often provide a danger to those in the sky and on the ground but in a very different way than the Internet of Things. *See, e.g.*, Michael S. Schmidt & Michael D. Shear, *Drones Hover Above, Seen But Not Halted*, N.Y. TIMES (Jan. 30, 2015), http://www.nytimes.com/2015/01/30/us/for-super-bowl-and-big-games-drone-flyovers-are-rising-concern.html (last visited June 16, 2015) (describing the security system at a major league baseball game that used radar to scan the sky for drones) (on file with the Washington and Lee Law Review).

20. While the acquisition of information by private companies, through surveillance, exchange, or sale can be just as troubling, that will be left for another article.

criminal and civil penalties based on the information, as well as conduct further reasonable searches and seizures.[21]

Governments can access information directly or with the knowing or unknowing assistance of private entities. The government–technology company "partnership" has long established roots stretching back to the Cold War in the mid-20th century, as well as the war on terrorism.[22] Instead of just using individuals to act as confidential informants as it mostly did several decades ago, the government also has been increasingly using private technology and phone companies, such as AT&T,[23] to tap into terabytes of information and serve in the same capacity.[24] These companies have become a new wave of informants.

Another government strategy has been to encourage companies, such as Google and Apple, to leave "back doors" or

---

21. *What Does the Fourth Amendment Mean?*, U.S. CTS., http://www.uscourts.gov/about-federal-courts/educational-resources/about-educational-outreach/activity-resources/what-does-0 (last visited Sept. 5, 2015) (explaining that the Fourth Amendment prohibits only unreasonable searches and seizures) (on file with the Washington and Lee Law Review)

22. *See* David Sanger & Nicole Perlroth, *Obama Heads to Security Talks Amid Tensions*, N.Y. TIMES (Feb. 13, 2014), http://www.nytimes.com/2015/02/13/business/obama-heads-to-security-talks-amid-tensions.html (last visited June 16, 2015) (noting a "long history of quiet cooperation between Washington and America's top technology companies") (on file with the Washington and Lee Law Review); Trevor Timm, *Building Backdoors Into Encryption Isn't Only Bad For China, Mr. President*, THE GUARDIAN (Mar. 4, 2015, 11:15 AM), http://www.theguardian.com/commentisfree/2015/mar/04/backdoors-encryption-china-apple-google-nsa (last visited June 16, 2015) (criticizing the U.S. government because the NSA and FBI are pushing for a law that requires technology companies to create encryption keys for the U.S. government while condemning China's plan to require technology companies to do the same) (on file with the Washington and Lee Law Review).

23. Julia Angwin et al., *NSA Spying Relies on AT&T'S 'Extreme Willingness to Help'*, PROPUBLICA (Aug. 15, 2015) https://www.propublica.org/article/nsa-spying-relies-on-atts-extreme-willingness-to-help (last visited Sept. 5, 2015) (reporting that newly disclosed documents show the relationship between the NSA and AT&T is "unique and especially productive") (on file with the Washington and Lee Law Review).

24. Edward Snowden, *Edward Snowden: The World Says No to Surveilance*, N.Y. TIMES (June 4, 2015), http://www.nytimes.com/2015/06/05/opinion/edward-snowden-the-world-says-no-to-surveillance.html (last visited Sept. 5, 2015) (recounting the nation's reaction to "the revelation that the National Security Agency had been making records of nearly every phone call in the United States") (on file with the Washington and Lee Law Review).

"keys" to its encrypted software for government use.[25] Through this strategy, the government has been able to "stockpile flaws in software—known as zero days—for future use against adversaries."[26] This stockpiling apparently allowed the NSA to tap into traffic between Google's servers because of a security flaw.[27]

An additional method the government can deploy to obtain information is the silent subpoena. It is silent because the subject does not know about its use due to secrecy concerns. The subpoena is all that is needed to reap reams of data.[28]

This Article examines the complex and significant constitutional implications of the government acquisition and use of information obtained through self-cybersurveillance. The Article argues that unless models of consent and privacy are changed, outdated legal rules will fail to protect individuals from the state in fundamental ways. The acquisition and use of advanced technology in the digital age can overcome privacy and constitutional barriers, including the separation of powers doctrine and the Third and Fourth Amendments.

The Article further suggests that to safeguard rights of privacy, constitutional boundaries must be tailored to the digital world. The need for enforcement is especially apparent in the emerging area of self-cybersurveillance. The concepts of Fourth Amendment privacy and consent, for example, have undergone considerable socio-cultural change in the last decade, while the

---

25. *See* Sanger & Perlroth, *supra* note 22 (discussing top technology companies' resistance to U.S. government efforts to force technology companies to install back doors or encryption keys in their products so the government can gain access).

26. *Id.*

27. *See id.* (noting reports of the NSA's interception of email traffic moving between Google and Yahoo servers). But the relationship appears to be troubled. According to the cybersecurity coordinator for the Obama Administration, Michael Daniel, "American firms are increasingly concerned about international competitiveness, and that means making a very public show of their efforts to defeat American intelligence gathering by installing newer, harder-to-break encryption systems and demonstrating their distance from the United States government." *Id.*

28. Companies are trying to circumvent these subpoenas by creating encrypted technology "that the firms themselves cannot break into—meaning they cannot turn over emails or pictures, even if served with a court order." *Id.*

controlling case law is much older.[29] The third-party doctrine,[30] which provides a bright line of all-or-nothing privacy for information disclosed to a third party under the Fourth Amendment, has swallowed up much of the discussion about the nuances and different types of consent in a digital world.[31] Without sufficient safeguards against indiscriminate surveillance and disclosure,[32] misuses will be inevitable and invisible, putting our system of checks and balances at risk.

II. Background

A. "Traditional" Surveillance

"Surveillance" means the close scrutiny or observation of others. It has occurred for centuries. In the 20th century, surveillance generally occurred in a physical world of walls and doors. Government or private surveillance used actual trackers, such as police officers, informants, and private detectives. The shadowy engagements of surveillance of spies and criminals created an entire vernacular, including "tailing," "stakeouts," and "observation posts." For surveillance to succeed, an element of

---

29. *See* United States v. Jones, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring) (asserting that the third-party doctrine is ill-suited to the digital age because people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks).

30. *See* John Villasenor, *What You Need to Know About the Third-Party Doctrine*, THE ATLANTIC (Dec. 30, 2013) http://www.theatlantic.com/technology/archive/2013/12/what-you-need-to-know-about-the-third-party-doctrine/282721/ (last visited June 20, 2015) (tracing the Supreme Court's development of the third-party doctrine) (on file with the Washington & Lee Law Review).

31. *See* Orin Kerr & Greg Nojeim, *The Data Question: Should the Third-Party Records Doctrine Be Revisited?*, A.B.A. J. (Aug. 1, 2012, 9:20 AM), http://www.abajournal.com/magazine/article/the_data_question_should_the_third-party_records_doctrine_be_revisited/ (last visited June 16, 2015) (providing a debate between two scholars about the merits of the third-party doctrine) (on file with the Washington and Lee Law Review).

32. To this end, limited, graduated disclosure of information should be recognized, and information boundaries both in time and place should be adopted, particularly if information ends up in the government's control. That is, limited disclosures should require opt-ins for further disclosure, not opt-outs, and gradations of third party access should not be taken as a complete negation of privacy rights.

secrecy generally was essential.[33] The agent who tailed a suspect, or the private detective who followed an allegedly unfaithful spouse, required secrecy to catch the suspect in some incriminating position.

Government surveillance used agents to physically observe suspicious persons,[34] often for crime interdiction. Surveillance frequently implicated the Fourth Amendment, given that considerable evidence was often obtained from that surveillance for use in subsequent prosecutions.[35]

Self-surveillance, on the other hand, was an oxymoron, a contradiction in terms. People would take family pictures for albums or film home movies, but generally without sufficient detail or sustained time to constitute surveillance. Diaries, for example, often captured life highlights or lowlights—but were not running narratives of the minute-by-minute existence of the points in between that yielded a time-lapse analysis of a person's life. Those gaps were part of memory and how we understood time—at least before the videotape, electronic medical records, or other instruments that could track accurately and unobtrusively over time.

When self-surveillance occurred, the surveilling generally was entirely private. Some diaries, for example, were locked with their own keys, and other diaries were just locked away in a private place, like a drawer or cabinet. Even photos or videos were stored in the home for use with family and sometimes friends, but not generally shared with strangers or the public.

---

33. *See, e.g.*, United States v. U.S. Dist. Court, 407 U.S. 297, 319 (1972) ("Secrecy is the essential element of intelligence gathering . . . .").

34. *See* Kenneth E. Weinberg, *Cryptography: "Key Recovery" Shaping Cyberspace (Pragmatism and Theory)*, 5 J. INTELL. PROP. L. 667, 694–98 (1998) (contending that technological advances eliminated the physical barriers to surveillance).

35. *See, e.g.*, United States v. Fischer, 38 F.2d 830, 830 (M.D. Pa. 1930) (considering evidence obtained by law enforcement officials while they physically observed the defendant from a position directly outside his house).

B. Modern Self-Surveillance and the Internet of Things

"You already have zero privacy—get over it." Scott McNealy[36]

In recent years, the opportunities for self-surveillance have grown exponentially.[37] Until the digital era, things or objects were mostly unifunctional. For example, a watch told time and glasses were used to see more clearly. The form of objects often described their function, such as hammers and nails. The objects were not "smart" like people, in any sense of the word—they could not think, evaluate, adapt, or display judgment or problem solving abilities. Unlike people, they could not create illusions in what they are or what they do. Yet, these distinctions between people and things are dissolving, especially today with the advent of interconnected and algorithm-adaptable things. The dissolution of learning capabilities between humans and devices has many implications, particularly for privacy.

Within five to ten years, there likely will be a fully operational "Internet of Things," where "smart" devices will connect to each other,[38] provide a multitude of data-driven opportunities, and create what some predict will be a fourteen trillion dollar economy[39] affecting every aspect of a person's life. As one M.I.T.

---

36. *See* Polly Sprenger, *Sun on Privacy: 'Get Over It'*, WIRED (Jan. 26, 1999), http://archive.wired.com/politics/law/news/1999/01/17538 (last visited Sept. 5, 2015) (noting that Scott McNealy is the CEO of Sun Microsystems) (on file with the Washington and Lee Law Review).

37. Some have the opportunities to surveil others, from spywear or other electronic means, even if they are not connected to the Internet. An individual who unplugs from the Internet in the safety and comfort of her own home, with the hope of controlling privacy, is not immune from tracking. Instead, she can be the subject of "Van Eck Phreaking," a cheap tool available for decades that can monitor and replicate what is on a computer screen remotely. Dan Seitz, *6 New Spy Technologies You Literally Can't Hide From*, CRACKED (Sept. 20, 2010), http://www.cracked.com/article_18771_6-new-spy-technologies-you-literally-cant-hide-from.html (last visited June 12, 2015) (on file with the Washington and Lee Law Review). This tool is not unreasonably expensive and can track both laptops and PCs. *Id.*

38. *See* Julianne Pepitone, *Google House: Tech Giant Spends Billions to Get Inside Your Home,* CNBC (Jan. 15, 2014, 6:11 AM), http://www.cnbc.com/id/101337483# (last visited June 16, 2015) (noting an M.I.T. professor's observation that Google's purchase of Nest Labs, a manufacturer of smart technology, will accelerate the progress toward home automation) (on file with the Washington and Lee Law Review).

39. *See id*. (stating that Cisco Systems estimates that the Internet of Things

professor noted, "The . . . first 20 years of the Web have been focused on human beings. The next era is going to be inanimate things."[40] These devices are "smart" insofar as they can adapt through programs and use data to improve efficiencies.[41] Remote operability will be commonplace—people will be able to remotely unlock the door to their home, turn off a kitchen appliance, and check the tire pressure in their car.[42] When a person awakens, there might be a smart thermostat that will automatically set the temperature to reflect activity in the house.[43] A smart meter will track the electricity used by occupants of the abode upon rising.[44] A smart toothbrush will track the quality of a person's tooth

---

could generate $14.4 trillion over the next decade).

40. *Id*. (quoting Sanjay Sarma, Associate Professor of Engineering, M.I.T.).

41. *See, e.g.*, Steve Lohr, *Homes Try to Reach Smart Switch*, N.Y. TIMES (Apr. 22, 2015), http://www.nytimes.com/2015/04/23/business/energy-environment/homes-try-to-reach-smart-switch.html (last visited June 16, 2015) (stating a home owner trimmed his electricity bill by 40% after installing a smart thermostat) (on file with the Washington and Lee Law Review).

42. *See* Pepitone, *supra* note 38 (discussing automated technology).

43. *See Nest Thermostats*, *supra* note 11 (describing Nest thermostats that track heat and air conditioning consumption, sense when residents leave their home, and automatically adjust the temperature).

44. *See, e.g.*, Marc Levy, *'Smart' Power Meters Track Electricity Use*, NBC NEWS (May 5, 2008, 1:39 PM), http://www.nbcnews.com/id/24459145/ns/technology_and_science-innovation/t/smart-power-meters-track-electricity-use/#.VYc251VViko (last visited June 16, 2015) (discussing the advantages of smart electricity meters that track the flow of electricity into homes) (on file with the Washington and Lee Law Review). In the early morning, a smart electric meter can track electricity consumption, from unusual surges in use to where in the house the source of usage originates. *See, e.g.*, Sunil Mallya, Entracker: Energy Tracker for Homes (Spring 2011) (unpublished M.S. Thesis, Brown University) (on file with the Brown University Library), *available at* https://cs.brown.edu/research/pubs/theses/masters/2011/mallya.pdf (detailing the design and functionality of a smart electric meter that tracks the electricity usage of each device in the household, rather than the household's aggregate consumption of electricity). A home's smart thermostat can track how much heat or air conditioning is being used, and when the thermostat should be adjusted. *See Nest Thermostats*, *supra* note 11 (describing smart thermostats). When everyone leaves the house, less energy is required and the thermostat can adjust automatically. *Id.* These patterns can be stored and utilized for future reference. *See Thermostat Guide*, NEST, https://developer.nest.com/documentation/cloud/thermostat-guide/ (last visited June 16, 2015) (explaining the Nest thermostat is "continuously learning about usage patterns in the home to optimize comfort and save energy") (on file with the Washington and Lee Law Review).

brushing.[45] The cell phone can be tracked up to every seven seconds to ensure it has the preferred location for cell tower reception.[46] When a user decides to go shopping, the cell phone permits retail stores to track its customers' location in and around the store.[47]

Connected persons also will have wearable technology. These people can check on their smart watches to determine what appointments they have for the day, what the stock market is doing at that time, or what the weather forecast will be.[48] When people observe an interesting situation, they might activate the real-time video feature of the smart glasses they are wearing.[49]

---

45. *See* Emma Bazilian, *Toothbrush, a Mini Drone and More,* ADWEEK (Mar. 11, 2015), http://www.adweek.com/news-gallery/advertising-branding/week-s-must-haves-smart-toothbrush-phone-charging-bracelet-and-more-163341 (last visited June 16, 2015) (noting how a smart toothbrush "connects to an app on your smartphone to track your brushing habits and provides real-time feedback on how to improve your routine") (on file with the Washington and Lee Law Review).

46. *See* Harkins, *supra* note 16, at 1877 (noting that cell phones connect with the nearest tower approximately every seven seconds). This information can provide a daily and sustained record of where that cell phone was twenty-four hours a day, seven days a week, and by inference, its possessor. *See id.* ("By gathering a sequential history of this cell site location information (CSLI), it is possible for the government to determine the whereabouts of your cell phone within approximately 200 feet every seven seconds."). That information could be obtained by Stingrays as well. Sam Adler-Bell, *Beware the "Stingray,"* US NEWS (Mar. 13, 2015), http://www.usnews.com/opinion/articles/2015/03/13/stingray-lets-police-spy-on-cellphones-and-they-want-to-keep-it-secret (last visited June 16, 2015) (on file with the Washington and Lee Law Review). A Stingray is a hand-held device that mimics cell phone towers, obtaining the same information. *Id.* Stingrays also are being used in some situations by police agencies for crime interdiction. *Id.*

47. *See* Stephanie Clifford & Quentin Hardy, *Attention, Shoppers: Store Is Tracking Your Cell*, N.Y. TIMES (Jul. 14, 2013), http://www.nytimes.com/2013/07/15/business/attention-shopper-stores-are-tracking-your-cell.html (last visited June 16, 2015) (discussing how retailers use signals from shoppers' cell phones to gather data, such as how long they spend in particular aisles or how long they look at merchandise before buying it) (on file with the Washington and Lee Law Review).

48. *See About*, SMARTWATCHPLUS, http://smartwatchplusios.appspot.com/index.htm (last visited June 16, 2015) (describing an app for a smart watch that provides these features) (on file with the Washington and Lee Law Review).

49. *See Atheer Showcases Real-Time Video Streaming Features for Gesture-Controlled Air Smart Glasses at 2015 HIMSS Conference, CTO Presents at IHA Workshop*, REUTERS (Apr. 14, 2015, 9:00 AM), http://www.reuters.com/article/2015/04/14/ca-atheer-idUSnBw145394a+100+BSW20150414 (last visited June 12, 2015) (describing the real-time video feature of Air Smart smart glasses) (on file with the Washington and Lee Law Review).

If people want to engage in an educational venture or just some entertainment before they leave the house, they can take advantage of emerging virtual reality, where 3-D headsets allow users to participate in holographic computing.[50] This computing will offer entertainment through gaming experiences and "field trips"[51] to exotic locations around the world. It also will offer technical and customer support, individuals who can be beamed to the wearer's view, permitting support personnel to share an internal home view.[52]

The information generated from the connected devices is not readily apparent and often is provided based on "soft consent," meaning an implicit acquiescence to sharing it with others. This consent extends from a check of the box on a website,[53] to the implicit understanding that once information is given to a third party, it can be shared with or sold to others.[54]

All electronic devices can be tracked even when not connected to the Internet because they emit radio waves.[55] Load monitoring, for example, allows devices to be remotely tracked when being used, providing information about the particulars of usage.[56] This

---

50. *See* Dan Kedmey, *Virtually Real: Microsoft Joins the Crowd Betting on 3-D Headsets*, TIME, Feb. 9, 2015, at 12 (calling the headset that enables holographic computing "the latest sign of how tech giants foresee a 3-D future").

51. *See id*. ("Teachers in virtual-reality-equipped classrooms could lead students on digital field trips to the rain forest or to witness the Battle of Waterloo.").

52. *See id*. (predicting that the 3-D headset will revolutionize customer support systems by allowing experts to see a customer's problem and walk him through fixing it).

53. *See, e.g.*, Michael L. Rustad & Maria Vittoria Onufrio, *Reconceptualizing Consumer Terms of Use for a Globalized Knowledge Economy*, 14 U. PA. J. BUS. L. 1085, 1112–13 (2012) (discussing terms of use agreements on social networking websites, which, after a user checks a box to assent, often waives a user's rights to user-generated content).

54. *See* Villasenor, *supra* note 30 (explaining the third-party doctrine that deems information shared with a third party outside the protection of the Fourth Amendment).

55. *See* Seitz, *supra* note 37 ("All electronics give off radio waves . . . . [T]he right tools can detect the waves given off by your monitor from afar and recreate what's being displayed on it.").

56. *See* Mario E. Berges et al., *Enhancing Electricity Audits in Residential Buildings with Nonintrusive Load Monitoring*, 14 J. INDUS. ECOLOGY 844 (2010) (stating that Nonintrusive Load Monitoring is a technique for deducing the power consumption and operational schedule of individual electricity loads in a

occurs, for example, through Nonintrusive Appliance Load Monitoring (NALM), which remotely tracks electricity usage of kitchen and other household appliances.[57]

Cars will provide another inflection point for obtaining information, although not from outward appearances. An occupant who gets into her car with tinted windows and no knowingly exposed information, such as bumper stickers or car decals, might assume there is at least some amount of anonymity once the doors close. Even without an external GPS device surreptitiously placed on a car, which occurred in the 2012 Supreme Court case, *Jones v. United States*,[58] that is increasingly not the case, cars have black boxes containing a device that measures various statistics about the operation of the car.[59] The device tracks miles traveled, speeds,

---

building).

57. *See* Michael Zeifman & Kurt Roth, *Nonintrusive Appliance Load Monitoring (NAILM): Promise and Practice*, DEP'T OF ENERGY (Mar. 1, 2012), http://energy.gov/sites/prod/files/2013/12/f6/nonintrusive_load_monitor.pdf (last visited July 18, 2015) (explaining how NALM tracks electricity usage) (on file with the Washington and Lee Law Review);

6 New Spy Technologies You Literally Can't Hide From, BX, http://slumz.box den.com/f610/6-new-spy-technologies-you-literally-cant-hide-from-1831507/ (last visited July 18, 2015)

> Once upon a time if a power company wanted to get a sense of how a household was using electricity, they'd have to get permission and attach sensors to things like your refrigerator or hot water heater to see how much each one is taxing the system moment to moment. NALM, on the other hand, can simply monitor the current as it runs through your house, from outside your house, and detect the exact signature of any device you own, at any given time. In Japan, they've designed a . . . 'neural network' of computers that can deduce exactly what electronic devices you're using via a Skynet-like pattern recognition. From that, it knows how long you've been in the shower, when you watch TV or use the computer.

(on file with the Washington and Lee Law Review).

58. Jones v. United States, 132 S. Ct. 945, 949 (2012) (holding the installation of a GPS device on the undercarriage of a citizen's vehicle and the use of that device to monitor the vehicle is a search within the ambit of the Fourth Amendment).

59. *See* Kim Komando, *Your Car's Hidden "Black Box" and How to Keep It Private*, USA TODAY (Dec. 26, 2014, 7:00 AM), http://www.usatoday.com/story/ tech/columnist/komando/2014/12/26/keep-your-car-black-box-private/20609035/ (last visited June 16, 2015) ("Since the early 2000s, the National Highway Traffic Safety Administration has been collecting black box information to get a better picture of the circumstances surrounding car accidents.") (on file with the Washington and Lee Law Review).

and other pertinent information about the vehicle.[60] This information is obtainable by car manufacturers,[61] ostensibly to track their products.[62]

If the car is traveling on the road, tag readers also can track it.[63] In Jackson, Mississippi, for example, the police are using automatic tag readers, as well as facial recognition software.[64]

Other places open to the public yield data streams.[65] Many people will stop during the day at a health club or gym to work out, participate in an exercise class, or to swim. While there, individuals can obtain health-related information through a heart-rate monitor or a device that tracks not only their heart rate, but

---

60. *Id*

61. *Id.*

62. *See* David Uris, *Big Brother and a Little Black Box: The Effect of Scientific Evidence on Privacy Rights*, 42 SANTA CLARA L. REV. 995, 1002 (2002) (noting that engineers have utilized the data provided by black boxes to enhance the operation of airbag sensing systems).

63. *See* Craig Timberg, *License-Plate Cameras Track Millions of Americans,* WASH. POST (July 17, 2013), http://www.washingtonpost.com/business/technology/license-plate-cameras-track-millions-of-americans/2013/07/17/40410cd0-ee47-11e2-bed3-b9b6fe264871_story.html (last visited June 16, 2015) (explaining that license-plate readers can identify cars almost instantly and compare them against lists of vehicles that have been stolen or involved in crimes) (on file with the Washington and Lee Law Review).

64. *See* Andrew Blankstein, *Meet Mega-Cops—High-Tech Crime Gear Transforms Police Work*, NBC NEWS (Feb. 8, 2014), http://www.nbcnews.com/news/investigations/meet-mega-cops-high-tech-crime-gear-transforms-police-work-n23841 (last visited June 16, 2015) (describing technological advances in policing) (on file with the Washington and Lee Law Review). Many officers now are equipped with on-body police video cameras. *Id.* The data derived from this equipment allows police to engage in "predictive policing," software that helps determine the allocation of resources to prevent or minimize future crimes. *Id.*

65. If a person plays a game, such as chess or scrabble, it is no longer just a game, especially if it is located on a cell phone. Instead, they are portals to information. Today, people might play *Angry Birds*, *Words With Friends*, *Minecraft, Clash of Clans*, and thousands of other games offered as phone applications. These applications accumulate considerable information about their users, both for the developers of the apps and advertisers. *See* Stephen Braun & Michael Liedtke, *Report: Spies Use Smartphone Apps to Track People*, YAHOO! NEWS (Jan. 27, 2014), http://news.yahoo.com/report-spies-smartphone-apps-track-people-190434189.html (last visited June 16, 2015) (describing tracking based on app use) (on file with the Washington and Lee Law Review). In addition, based on leaks, it appears that the NSA and other spy agencies in the United States and Great Britain can access large amounts of personal data through the apps, including information about location, political affiliation, and even sexual orientation. *Id.*

also how many steps they take or calories they burn.[66] These devices gather and store the data, which is then uploaded to a computer site and aggregated with other data.[67]

C. Linking Self-Surveillance to the Government—Public–Private Partnerships and the New Informants

1. A Significant Source of Government Information: Companies Tracking Individuals

Commercial companies tracking individuals provide a fertile source of information for the government. Much of this tracking is based on the implicit acquiescence by users of websites.[68] In an interconnected world, just about everything we do, from personal hygiene, to finances, to at-home free time preferences, is on the "grid"—connected to others in one or more ways with our implicit assent. To make appointments with doctors, utilize online banking privileges, or follow friends on Facebook, users must acquiesce to disclosure policies set by the website—policies that often are filled with fine print and run on for paragraphs, if not pages.[69] While refusal to comply is an option, the resulting consequences can include inconvenience or worse—separation from a social environment or culture.

Tracking of people often occurs on the Internet through private company "cookies."[70] Cookies are a form of identification

66. *See, e.g.*, Fitbit, *supra* note 12 (advertising a watch that "tracks every part of your day—including activity, exercise, food, weight, and sleep—to help you find your fit").

67. *See id.* (explaining that Fitbit tracks one's progress so the user can view it online or from a mobile device).

68. *See* Allyson W. Haynes, *Online Privacy Policies: Contracting Away Control Over Personal Information?*, 111 PENN. ST. L. REV. 587, 597 (2007) (highlighting that most websites' terms of use agreements state that users consent to the agreement by simply using the website).

69. *See id.* at 588 ("[M]ost studies show that, while consumers are increasingly concerned about the privacy of their personal information, they are still not likely to read—much less understand—online privacy.").

70. *See All About Cookies*, ALLABOUTCOOKIES.ORG, http://www.allaboutcookies.org (last visited Mar. 10, 2015) ("Cookies are usually small text files, given ID tags that are stored on your computer's browser directory or program data subfolders.") (on file with the Washington and Lee Law Review).

tags that are delivered through Web browsers when a computer user visits a website. Sometimes, third parties place cookies or tags on computers as well; these are often placed by advertisers with banners or ads on the visited sites.[71] Individuals can remove cookies or block tracking, but unless a user acts with intentionality—and understands how these invisible trackers operate—the user will be subject to multiple cookies and the distribution of information to others.[72] The third parties who get some of the information shared by site owners—or who place what is known as third-party cookies on computers[73]—generally lurk in the shadows unseen.

The type of consent given for the access and gathering of site user information varies, from expressly checking a box,[74] to implicit acknowledgement through conduct, such as downloading site content or clicking a link on a site that leads to another site. In these situations, we generally provide consent to the site's rules to enter it.[75] We also have acquiesced, though, to tracking by third parties and the controllers of the site, perhaps in unseen ways, particularly with reference to what is done with information created by a site visit. As one commentator has noted:

> It's no secret that we're monitored continuously on the Internet. Some of the company names you know, such as Google and Facebook. Others hide in the background as you move about the Internet. There are browser plugins that show you who is tracking you. One Atlantic editor found 105 companies tracking him during one 36-hour period. Add data from your cell phone (who you talk to, your location), your credit cards (what you buy, from whom you buy it), and the dozens of other times you

71. *See id.* (explaining cookies' role in third-party advertisements on a website).

72. *See* Max Stul Oppenheimer, *Internet Cookies: When Is Permission Consent?*, 85 NEB. L. REV. 383, 384 (2006) (explaining that current browsers accept cookies by default and that cookies can be used to monitor and record transactions between a user's computer and the server).

73. *See id.* at 386 n.15 (noting how a third-party cookie either originates on or is sent to a website different than the one the user is currently viewing).

74. *See* Register.com, Inc. v. Verio, Inc., 356 F.3d 393, 403 (2d Cir. 2004) (noting that "contract offers on the internet often require the offeree to click on an 'I agree' icon").

75. *See* Haynes, *supra* note 68, at 597 (explaining that viewing a website can bind the user to the website's terms of use contract).

> interact with a computer daily, we live in a surveillance state beyond the dreams of Orwell.[76]

Sending and receiving of emails also creates traceable metadata.[77] Internet Service Providers (ISPs) usually store such metadata that can be transferred or sold.[78] Private companies and the government can track the email metadata—where and when the email was created and who were the parties to it.[79]

Commercial tracking of current or potential customers often occurs in the retail industry, both on the Internet and in person. When customers enter a store, for example, the store can track physical movements through cell phones and thereby determine shopping habits, from which floors and departments the customers visit, to how long and how often the customers visit.[80] Advertisers, of course, want to know about customer habits. Google Plus, for example, is a social network, but it provides a trove of personal information because it aggregates all Google products into one account, including Gmail, Google Maps, and YouTube. This allows Google to track the habits of its customers.[81]

---

76. Bruce Schneier, *Do You Want the Government Buying Your Data From Corporations?*, THE ATLANTIC (Apr. 30, 2013), http://www.theatlantic.com/technology/archive/2013/04/do-you-want-the-government-buying-your-data-from-corporations/275431/ (last visited June 16, 2015) (on file with the Washington and Lee Law Review).

77. *See* Mike Breen, *Nothing to Hide: Why Metadata Should Be Presumed Relevant*, 56 U. KAN. L. REV. 439, 442–43 (2008) (providing examples of metadata created by sending emails, such as the recipients of blind carbon copies).

78. *See* Paul Ohm, *The Rise and Fall of Invasive ISP Surveillance*, 2009 U. ILL. L. REV. 1417, 1436 (2009) (predicting that the majority of ISPs will soon capture everything their users do online and sell this information to third parties).

79. *See* Shane Scott & Jonathan Wiseman, *Earlier Denials Put Chief in Awkward Position*, N.Y. TIMES (June 11, 2013), http://www.nytimes.com/2013/06/12/us/nsa-disclosures-put-awkward-light-on-official-statements.html?hp&_r=0 (last visited June 16, 2015) (reporting on the Snowden disclosures and Eric Clapper's statement that he gave the "least untruthful answer" he could when asked whether the NSA collected data on hundreds of millions of Americans) (on file with the Washington and Lee Law Review).

80. *See* Clifford & Hardy, *supra* note 47 (stating that retailers use signals from shoppers' cellphones "to learn information as varied as their sex, how many minutes they spend in the candy aisle and how long they look at merchandise before buying it").

81. *See* Claire Cain Miller, *The Plus in Google Plus? It's Mostly for Google*, N.Y. TIMES (Feb. 14, 2014), http://www.nytimes.com/2014/02/15/technology/the-plus-in-google-plus-its-mostly-for-google.html (last visited June 16, 2015) (noting

The tracking of customers can occur, even outside of stores, through stationary objects like garbage cans.[82] Smart garbage cans, costing in excess of $45,000, were placed in various spots during the London Olympics to track traffic passing by the cans.[83] These Renew Pods, with Orb technology, were kept operational after the Olympics and continued their tracking for several years, collecting anonymized information about traffic patterns and potential customers.[84] According to one report, the bins tracked passersby to study their shopping habits.[85]

Companies have begun using radio frequency identification technology (RFID) to track items from a considerable distance.[86] This technology implants a small chip in the object so it can be monitored at any time.[87] In 2003, for example, Wal-Mart embedded

---

that Google Plus has 540 million monthly users and even if they do not visit the social network site, their shopping habits can be tracked for advertisers' use) (on file with the Washington and Lee Law Review).

82. *See* Rachel Savage, *Snooping Garbage Bins in City of London Ordered to Be Disabled*, BLOOMBERG (Aug. 12, 2013, 10:06 AM), http://www.bloomberg.com/news/articles/2013-08-12/snooping-garbage-bins-in-city-of-london-ordered-to-be-disabled (last visited June 16, 2015) ("Technology in the bins 'detects smartphones by proximity, speed, duration and manufacturer.'" (citation omitted)) (on file with the Washington and Lee Law Review).

83. *Id.*

84. The Chief Executive Office of Renew described what the cans did: "During our current trials, a limited number of pods have been testing and collecting anonymized aggregated [Media Access Control] addresses from the street and sending one report every three minutes concerning total footfall data from sites." *Id.*

85. *See id*. (explaining that the garbage bins collect data about the shopping habits of people that pass by, so the LCD screens on the bins display targeted adds); James Vincent, *(Updated) London's Bins Are Tracking Your Smartphone*, THE INDEPENDENT (Aug. 9, 2013), http://www.independent.co.uk/life-style/gatdgets-and-tech/news/updated-londons-bins-are-tracking-your-smart phone-8754924.html (last visited June 16, 2015) (explaining that the data from the bins could allow companies "to track which stores individuals visit, how long they stay there ('linger time') and how loyal customers are to particular shops") (on file with the Washington and Lee Law Review).

86. *See* David R. Hancox, *Using RFID Technology to Enhance Corporate Effectiveness,* INTERNAL AUDITOR (Apr. 1, 2006), https://iaonline.theiia.org/using-rfid-technology-to-enhance-corporate-effectiveness (last visited June 16, 2014) (contending that companies should place RFID tags on equipment and inventory because it will reduce tracking costs by providing up-to-date, accurate, and timely data) (on file with the Washington and Lee Law Review).

87. *See id.* ("RFID tags can be embedded into or onto objects without the knowledge of the individual obtaining or holding these items. This has already

lipstick containers with RFID technology in its Broken Arrow, Oklahoma store.[88] The containers could be tracked from seven hundred miles away by researchers, including a video monitor of the consumers handling the products.[89]

While private companies, as well as the government, have contributed to the crumbling of the private sphere through various methods of tracing and tracking, defenses are also being erected. Encryption has been one of the primary defensive tactics to prevent the access to and gathering of private information.[90] It is designed to prevent third parties from accessing the computer through back-doors, but these safeguards are not impregnable and even are sometimes intentionally weak, making them easier to breach. Information on a site can be readily downloaded surreptitiously with Web crawlers and other tools.

2. Government Use of Private Companies

The federal government links up with the information produced by self-cybersurveillance by enlisting the assistance of private companies. Government agencies, including the NSA, CIA, FBI, and some branches of the military are involved in tracking.[91]

---

been done by home and personal products company Gillette, which placed hidden tags inside Mach3 razor blade packages . . . .").

88. *See* Laura Hildner, *Defusing the Threat of RFID: Protecting Consumer Privacy Through Technology-Specific Legislation at the State Level*, 41 HARV. C.R.-C.L.L. REV. 133, 133 (2006) (noting that RFID technology has been called "the next big thing").

89. *Id.* The incident became known as the "Broken Arrow Affair." *Id.* The use of RFID technology has persisted, although it has been controversial. *Id.* at 134.

90. *See* J.D. Meier et al., *Threats and Countermeasures*, MICROSOFT (June 2003), https://msdn.microsoft.com/en-us/library/ff648641.aspx (last visited June 15, 2015) (describing encryption as one of the countermeasures that can protect a computer user from information disclosure) (on file with the Washington and Lee Law Review).

91. *See* Michael Riley, *U.S. Agencies Said to Swap Data with Thousands of Firms*, BLOOMBERG (June 15, 2013, 12:01 AM), http://www.bloomberg.com/news/articles/2013-06-14/u-s-agencies-said-to-swap-data-with-thousands-of-firms (last visited June 16, 2015) (stating that the NSA, CIA, FBI, and branches of the U,S. military have agreements with companies to gather data that might seem innocuous but could be highly useful in the hands of U.S. intelligence or cyber-warfare units) (on file with the Washington and Lee Law Review).

This leveraging of private efforts creates efficiencies and synergies for the government and sometimes the private companies as well.

The critical relationship between government and private business began to surface after the Snowden revelations, but it is nothing new.[92] Companies began working with the government to crack codes as far back as the Cold War.[93]

Much of the partnering has appeared to be based on "mutual interest."[94] These interests included weak encryption on software products that the government could easily break.[95] By leaving in back doors or allowing the government to stockpile "zero-day flaws," meaning flaws in software for offensive or defensive government use, government security agencies accumulated far greater quantities of data.[96] With the technology companies holding a key to their software, the government could likely obtain a key as well.[97]

Companies often worked so closely with the government that members of the government were sometimes given physical access to the companies:

---

92. The role of private companies has come under intense scrutiny since his disclosure in June 2013 that the NSA is collecting millions of U.S. residents' telephone records and the computer communications of foreigners from Google Inc. and other Internet companies under court order. Ryan Gallagher, *NSA Collecting Phone Records for Millions of U.S. Verizon Customers*, SLATE (June 6, 2013, 10:20 AM), http://www.slate.com/blogs/future_tense/2013/06/06/nsa_verizon_phone_records_national_security_agency_order_collects_metadata.html (last visited June 16, 2015) (on file with the Washington and Lee Law Review).

93. "The Cold War" refers to the tensions between the Soviet Union and Western countries after World War II.

94. *See* Sanger & Perlroth, *supra* note 22 ("The long history of quiet cooperation between Washington and America's top technology companies—first to win the Cold War, then to combat terrorism—was founded on the assumption of mutual interest.").

95. *See id.* (discussing zero-day flaws).

96. *See id.* (noting the tension between technology companies and the government due to "the government's desire to stockpile flaws in software—known as zero days—to develop weapons that the United States can reserve for future use against adversaries").

97. *Cf. id.* ("The F.B.I., the intelligence agencies and David Cameron, the British prime minister, have all tried to stop Google, Apple and other companies from using encryption technology that the firms themselves cannot break into—meaning they cannot turn over emails or pictures, even if served with a court order.").

> Thousands of technology, finance and manufacturing companies are working closely with U.S. national security agencies, providing sensitive information and in return receiving benefits that include access to classified intelligence . . . These programs, whose participants are known as trusted partners, extend far beyond what was revealed by Edward Snowden, a computer technician who did work for the National Security Agency.[98]

Given that today's tracking often results from the commercial efforts of private technology or retail companies, and now our own efforts to self-surveil every aspect of our lives, the governmental collection, storage, and analysis of data can seem almost incidental. Indeed, much of the bulk collection is not effectuated directly by the government, even though the government has a massive database of every call made inside the United States, but rather by the private telecommunications companies.[99] The government has used the data stored by the telecommunications companies in addition to the data it collected through its own agencies.[100] It is not only the telecommunications companies that participate in these relationships:

> Makers of hardware and software, banks, Internet security providers, satellite telecommunications companies and many other companies also participate in the government programs. In some cases, the information gathered may be used not just to defend the nation but also to help infiltrate computers of its adversaries.[101]

Especially over the past several years, companies have realized—as did the population at large after the Snowden leaks—that government requests for information could be "an intrusion into the privacy of their customers and a risk to their businesses."[102] Some companies have changed paths as a result of this realization.

---

98. Riley, *supra* note 91.

99. *See id.* ("Thousands of technology, finance and manufacturing companies are working closely with U.S. national security agencies, providing sensitive information and in return receiving benefits that include access to classified intelligence.").

100. *See* Sanger & Perlroth, *supra* note 22 (stating that intelligence agencies buy information about flaws in widely-used hardware and software and do not reveal the flaws to manufacturers).

101. Riley, *supra* note 91.

102. Sanger & Perlroth, *supra* note 22.

III. Implications of Self-Cybersurveillance

A. The Downward Slope of Privacy Protection

As self-cybersurveillance grows in all directions and the accompanying "soft consent" to share data with third parties expands, the amount of data obtained by the government likely will increase exponentially. This flow of exposed information will lead to further erosion of the private sphere in fact and as a guiding principle.

Under current interpretations of the Fourth Amendment and the prevailing third-party doctrine, more and more information will be treated as totally exposed to the public and obtainable by the government without any hurdles whatsoever. The view of privacy under the third-party doctrine as an all-or-nothing marker[103] is reinforced in today's interconnected society. A culture of sharing, from medical records,[104] to school information,[105] to personal "selfies,"[106] is the rule, not the exception.

---

103. *See* Erin Smith Dennis, *A Mosaic Shield: Maynard, the Fourth Amendment, and Privacy Rights in the Digital Age*, 33 CARDOZO L. REV. 737, 739 (2011) (explaining that third-party doctrine limits a court's ability to find any Fourth Amendment protections for information an individual shares with another). Some integral third parties include health care providers, accountants, and clergy. *Id.* at 751 n.92.

104. *See* Tara Culp-Ressler, *Big Data Companies Are Selling Lists of Rape Victims to Marketing Firms*, THINKPROGRESS (Dec. 19, 2013, 1:34 PM), http://thinkprogress.org/health/2013/12/19/3089591/big-data-%20health-data-mining/ (last visited June 16, 2015) ("So-called 'data brokers' are selling Americans' personal health information to marketers, according to a new report from the Senate Commerce Committee.") (on file with the Washington and Lee Law Review).

105. *See* Jordan Shapiro, *Your Kid's School May Have The Right To Sell Student Data*, FORBES (Jan. 24, 2014, 8:28 AM), http://www.forbes.com/sites/jordanshapiro/2014/01/24/your-kids-school-may-have-the-right-to-sell-student-data/ (last visited June 16, 2015) (highlighting that the Family Educational Rights and Privacy Act was revised in 2011, rendering the collection of student data to develop individualized education plans for students legal) (on file with the Washington and Lee Law Review).

106. *See* Julianne Pepitone, *Instagram Can Now Sell Your Photos for* Ads, CNN (Dec. 18, 2012, 6:14 PM), http://money.cnn.com/2012/12/18/technology/social/instagram-sell-photos/ (last visited June 16, 2015) (reporting Instagram's revised terms of use that allow business entities to pay Instagram to display users photos in connection with paid or sponsored content or promotions) (on file with the Washington and Lee Law Review). It is important to note that Instagram changed this policy due to public outcry. *Id.*

The permeation of a sharing culture greatly diminishes accepted understandings of privacy. Whether privacy is defined as the right to be left alone, autonomy, or something else altogether, control over intimate data undoubtedly is central to informational privacy. Despite that centrality, the protean nature of privacy norms within the current context has led to a loosening of control over important personal information.

If privacy includes freedom from disclosure of intimate information, the Internet of Things has invaded the one sanctuary that remains where communications are traditionally private—the home.[107] The seminal article by Samuel Warren and Louis Brandeis on privacy in 1890 noted that an individual's privacy includes the "right of determining, ordinarily, to what extent his thoughts, sentiments, and emotions shall be communicated to others."[108] This communicative control has been lost, or at least misplaced, in the ongoing digital revolution, where heartbeats and sleep patterns can be measured, packaged, and instantaneously shared with others.[109]

Thus, the impact of the Internet of Things affects the pre-digital public/private distinction as well. That distinction is tightly linked to physical spaces, including the home, curtilage,[110] or workplace. Given the current trend of information dissemination regardless of physical location, there is a very real possibility of the public/private dichotomy being set free from its physical moorings, with no real refuge for individuals, unless they choose to leave "the grid" of interconnected life—an extreme measure in today's age.

The argument that government access and use of information formerly protected by privacy will increase the security of our country is an unproven maxim. As one commentator has noted, "[l]iberty requires security without intrusion, security plus

---

107. If privacy is writ large as a check against government overreaching, it will no longer serve that purpose either.

108. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 198 (1890).

109. *See supra* Part II.B (describing modern self-surveillance and the Internet of Things).

110. The curtilage is the area immediately around the home, such as a porch, that is protected under Fourth Amendment privacy concepts. *See, e.g.*, United States v. Dunn, 480 U.S. 294, 300 (1987) (explaining that Fourth Amendment protections extend to a home's curtilage).

privacy."[111] There has been no empirical showing that greater intrusion necessarily leads to greater security.

The proposition that the potential for abuse will not increase because of greater secrecy in government acquisition of information also lacks support. The higher the level of secret intrusion, the fewer the checks and balances on any invasiveness, priming the pump for abuse. This secondary assumption, that the government will not abuse any information it receives, is untrue, as exemplified recently by the Internal Revenue Service and its abuse of some information it gathered.[112]

If the last bastion of local privacy, the home, continues to increase its multiple and regular connections to third parties,[113] steps must be taken to reinvent the security, autonomy, and creative space that privacy represents before it dissipates like air leaking out of a tire. Instead, safeguards can be erected to protect privacy as a concept and practice.

B. Proposed Safeguards

1. Adapt Existing Case Law

The predigital case law of the Supreme Court has mostly cabined privacy rights as an all-or-nothing commodity in a physical world of walls and doors. *Katz v. United States*,[114] decided in 1967, remains the seminal Supreme Court case determining what

---

111. Richi Jennings, *Google CEO: If You Want Privacy, Do You Have Something To Hide?*, COMPUTERWORLD (Dec. 11, 2009, 6:06 AM), http://www.computerworld.com/article/2468308/internet/google-ceo--if-you-want-privacy--do-you-have-something-to-hide-.html (last visited June 16, 2015) ("According to documents recently obtained by the American Civil Liberties Union, the Internal Revenue Service believes they have the authority to read the private e-mail messages, Facebook chats, and other online communications of Americans without obtaining a warrant.") (on file with the Washington and Lee Law Review).

112. Madison Ruppert, *IRS Claims They Can Read Your E-mail and Other Electronic Communications Without A Warrant*, ACTIVIST (Apr. 11, 2013), http://www.activistpost.com/2013/04/irs-claims-they-can-read-your-e-mail.html (last visited June 16, 2015) (discussing the IRS Search Warrant Handbook, and its conclusion that Americans have no privacy in online communications) (on file with the Washington and Lee Law Review).

113. *See supra* notes 37–45 and accompanying text (describing smart household devices that collect information about families).

114. 389 U.S. 347 (1967).

constitutes a search under the Fourth Amendment.[115] At the time it was handed down, it was seen as a progressive case that untethered the boundaries of the Fourth Amendment from physical spaces, protecting people, not places.[116] The *Katz* test, enunciated by Justice Harlan in his concurrence, had the potential for flexibility and adaptability to new technology.[117] Unfortunately, its promise has gone unfulfilled, with the Supreme Court reluctant to wade into an on-going digital revolution, instead sticking to *Katz* progeny that appear increasingly ossified.

One of the most significant of these progeny, *United States v. Miller*,[118] confronted the question of whether bank records accessed by the government were private under the Fourth Amendment.[119] The Court held that the records were not private, and in doing so differentiated bank records from private papers.[120] The Court said there was no expectation of privacy in bank records that were negotiable instruments intended as a part of a commercial transaction, rather than as a confidential communication.[121] Consequently, the Court found that the defendant had no Fourth Amendment interest that would protect him from the subpoena for the records.[122] Interestingly, many people do not discuss their finances even with friends, usually confiding in financial advisors.

---

115. *See* Daniel T. Pesciotta, *I'm Not Dead Yet: Katz, Jones, and the Fourth Amendment in the 21st Century*, 63 CASE W. RES. L. REV. 187, 188 (2012) (citing *Katz* as the seminal ruling that established as unconstitutional warrantless searches that encroach upon a citizen's reasonable expectation of privacy).

116. *See Katz*, 389 U.S. at 350–51 ("[T]he Fourth Amendment protects people, not places.").

117. *See id.* at 361 (Harlan, J., concurring) ("There is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as reasonable.").

118. 425 U.S. 435 (1976).

119. *See id.* at 437 (stating that the motion to suppress concerned checks and other bank records).

120. *See id.* at 440 ("On their face, the documents subpoenaed here are not respondent's 'private papers' . . . . Instead, these are the business records of the banks.").

121. *See id.* at 442 (explaining that "checks are not confidential communications but negotiable instruments to be used in commercial transactions").

122. *See id.* at 443 ("The depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government.").

The precise nature of finances often is held closely and confidentially, with many states acknowledging this confidentiality by recognizing an accountant-client privilege.[123]

Another important subsequent decision, *Smith v. Maryland,*[124] followed *Miller* and became an additional cornerstone of the third-party doctrine. In *Smith*, the Court held that pen registers were not within the privacy protected under the Fourth Amendment.[125] The facts of the case are significant, though, despite being obscured over time. In *Smith*, a person suspected of robbing a woman allegedly was calling the victim and threatening her.[126] To follow-up on this ongoing threat as well as investigate the robbery crime, the police obtained a pen register to trace the phone that was calling the victim.[127] The pen register was sought to stop ongoing criminal activity and, further, the police had reason to believe the phone calls were directly connected to the prior robbery.[128]

While *Katz, Smith*, and *Miller* have seemingly created a ceiling for the constitutional protection of information, these cases can still serve to safeguard informational privacy in the digital world. In *Katz*, the Court found that an outdoor phone booth provided a reasonable expectation of privacy against nonconsensual wiretapping.[129] Even though the phone booth was outdoors, and even though people could see into the phone booth, the fact that there were walls and doors on the booth provide for

---

123. *See* Alan W. Anderson & Elizabeth E. Brown, *Colorado's Accountant-Client Privilege*, 24 COLO. LAW. 283, 286 (1995) (noting that Colorado and many other states recognize an accountant-client privilege).

124. 442 U.S. 735 (1979).

125. *See id.* at 745 (finding that because there is no legitimate expectation regarding the phone numbers citizens dial, the installation of a pen register is not a search within the ambit of the Fourth Amendment).

126. *See id.* at 737 ("After the robbery, [the victim] began receiving threatening and obscene phone calls from a man identifying himself as the robber.").

127. *Id.*

128. *See id.* (noting that the man calling identified himself as the robber).

129. Katz v. United States, 389 U.S. 347, 353 (1967) ("The Government's activities in electronically listening to and recording the petitioner's words violated the privacy upon which he justifiably relied while using the telephone booth and thus constituted a 'search and seizure' within the meaning of the Fourth Amendment.").

reasonable privacy expectations.[130] Today, walls and doors have been replaced by encryption. Encrypted data sent over the Internet can be shielded by a similar set of expectations. The same expectations apply to password-protected communications, indicating both subjective and reasonable expectations of privacy.

Smith has been used to justify bulk metadata collection, particularly for phone calls.[131] The facts of *Smith*, however, are far removed from justifying bulk data collection, which provides for a horizontal collection approach—without any prior reasonable expectation of criminality in the data—and not a vertical approach building on prior reasonable suspicion. Bulk data collection is thus wholesale, not retail, in that there is no specific criminality that is underfoot, justifying police intrusion. Further, the information collected from innocent bystanders is exponentially greater than that which occurs from any one pen register.[132] The horizontal collection approach transforms the particularity requirement, not as matter of degree but rather as a fundamental shift in the nature of police activity. Even if the information contains no inherent indicia of privacy protection, the burden of collection and retention with mass collection should remain on the government because of the horizontal/vertical dichotomy.

Consequently*, Smith* and *Miller* do not lead inexorably to the dismantling of privacy for all things revealed to others, and should no longer be used for such a proposition. Further, not everyone agrees with the Supreme Court's all-or-nothing approach to privacy. Justice Thurgood Marshall, dissenting in *Smith v. Maryland*, stated: "Privacy is not a discrete commodity, possessed absolutely or not at all."[133] This statement becomes even more

---

130. *See id.* (explaining that fact that the listening device did not penetrate the wall of the booth had no constitutional significance).

131. *See* Joseph D. Mornin, *NSA Metadata Collection and the Fourth Amendment*, 29 BERKELEY TECH. L.J. 985, 987 (2014) (explaining that the Government relies on *Smith* to defend the constitutionality of its bulk data collection).

132. *See* James Ball, *NSA Collects Millions of Text Messages Daily in an 'Untargeted' Global Sweep*, THE GAURDIAN (Jan. 16, 2014, 1:55 PM), http://www.theguardian.com/world/2014/jan/16/nsa-collects-millions-text-messages-daily-untargeted-global-sweep (last visited Sept. 5, 2015) ("The National Security Agency has collected almost 200 million text messages a day from across the globe . . . .") (on file with the Washington and Lee Law Review).

133. Smith v. Maryland, 442 U.S. 735, 748 (1979) (Marshall, J., dissenting).

appealing as technology strips privacy away. As one commentator noted:

> But the idea that information exposed to others is no longer private has been oversold. Millions of Americans expect all sorts of things exposed to third parties remain private under state law. And as technology advances and the information we give to ISPs and telcos becomes more and more revealing, even federal courts are beginning to rethink whether Smith is the absolute rule the government claims it should be. . . . On its 35th birthday, Smith's vitality is on the decline, and that's a good thing.[134]

2. Reconstitute the Public–Private Distinction

There are those who argue there is nothing private in public anymore, and the extensive use of self-cybersurveillance and other evidence supports this position. Everyone is constantly connected, as evidenced by people texting in restaurants while eating, while watching films in theaters,[135] and while driving.[136] Cell phones permeate society, especially in public, as they allow individuals to be ready to take pictures at a moment's notice. Face recognition software also is in use, although mostly by private companies, such as Facebook.[137] Once pictures are posted on Facebook, for example,

---

134. Hanni Fakoury, Smith v. Maryland *Turns 35, But Its Health Is Declining*, ELECTRONIC FRONTIER FOUND. (June 24, 2014), https://www.eff.org/deeplinks/2014/06/smith-v-maryland-turns-35-its-healths-declining (last visited June 16, 2015) (on file with the Washington and Lee Law Review).

135. A shooting at a Florida movie theater occurred as a result of the victim texting in the darkened theater. Steve Almasy, *Dad's Texting to Daughter Sparks Argument, Fatal Shooting in Movie Theatre*, CNN (Jan. 13, 2014, 6:20 PM) http://www.cnn.com/2014/01/13/justice/florida-movie-theater-shooting/ (last visited June 16, 2015) (on file with the Washington and Lee Law Review).

136. Many states have moved to make texting while driving unlawful. Amy L. Brueckner, *Distracted Driving: How Technological Advancements Impede Highway Safety*, 115 PENN. ST. L. REV. 709, 722 (2011).

137. *See* Meagan Rose Dickey, *Facebook Wants to Add Your Profile Picture to Its Face Recognition Database*, BUS. INSIDER (Aug. 29, 2013), http://www.businessinsider.com/facebook-facial-recognition-database-2013-8 (last visited June 13, 2015) (stating Facebook is considering adding profile pictures to its facial recognition database in order to improve the accuracy of its "Tag Suggest" feature) (on file with the Washington and Lee Law Review).

they become part of a database of more than one billion photos.[138] The government also is developing its own face recognition software system that will be able to detect faces of up to 100 yards away.[139] In the skies, there are drones and eye-in-the-sky cameras, as well as closed circuit TV on land, and even drones underwater.[140] The Internet of Things has invaded the home space, creating little refuge for anyone using multifunctional connected devices—which is most of us.[141]

It is not the individual pieces of information that are the problem with mass disclosure, but rather the dismantling of the private sphere. The information derived from smart devices can be aggregated to reveal private personal preferences as well as habits—and lots of data about each.[142] They reveal our identities

---

138. *See Facebook Could Add Its One Billion Users' Profile Pictures to Photo Database—Meaning Even MORE Users Will Be Automatically Tagged*, DAILY MAIL (Aug. 29, 2013, 7:10 PM), http://www.dailymail.co.uk/news/article-2406204/Facebook-add-billion-users-profile-pictures-photo-database--meaning-users-control-social-network-recognizing-photos.html (last visited June 16, 2015) (noting that Facebook believes the move will improve privacy because users will know when pictures of them have been posted) (on file with the Washington and Lee Law Review).

139. This system is called the biometric optical surveillance system (BOSS). The drone, an unmanned aerial vehicle, not only can carry cargo, but can beam real-time pictures to remote pilots. While not in regular use in the United States, these are gaining a foothold and becoming more widespread, as recent rules on commercial-use drones reveal. Charlie Savage, *Facial Scanning is Making Gains in Surveillance*, N.Y. TIMES (Aug. 21, 2013), http://www.nytimes.com/2013/08/21/us/facial-scanning-is-making-gains-in-surveillance.html?_r=0 (last visited May 4, 2015) (on file with the Washington and Lee Law Review).

140. Eye-in-the-sky cameras, which are attached to the wings of aircraft and used to take pictures automatically, also provide surveillance. These cameras have been used for crime interdiction, including detecting burglaries in progress. Martha Neil, *Eye-in-the-Sky Surveillance a New Tool for US Cities; Is Spying Via Camera While Flying Too Prying?*, A.B.A. J. (Feb. 5, 2014, 10:45 PM), http://www.abajournal.com/news/article/eye_in_the_sky_surveillance_a_growing_reality_in_us_cities/ (last visited May 4, 2015) (on file with the Washington and Lee Law Review).

141. The extent of the surveillance and exposure in public to others indicates that there are limited, if any, reasonable expectations of privacy in public. But that does not tell the whole story. The idea of "public" as anything outside one's home excludes how much intrusiveness ought to be permitted outside the home. *See* Max Guirguis, *Electronic Visual Surveillance and the Reasonable Expectation of Privacy*, 9 J. TECH. L. & POL'Y 143, 150–51 (2004) (noting the effectiveness of advances in surveillance technology as a factor contributing to the decline in privacy expectations).

142. *See* Julia Angwin, *The Web's New Gold Mine: Your Secrets*, WALL ST. J.

and what we think about ourselves.[143] The companies and government can use this data in addition to data already on file to create unusually detailed pictures of the subjects they portray.[144]

The government, in particular, should not be allowed to gather data indirectly that it could not gather directly. The public/private distinction should be used to prevent the government from accessing and storing such private information permanently.[145] Devices using information to promote their functionality should not be used to transmit that information to third parties for unrelated purposes—and then transmit that information to the government for purposes purportedly related to crime interdiction without any reasonable basis for doing so.[146] If a smart thermostat is used to accommodate and maximize the efficiency of the heat and air conditioning process, for example, that does not mean the occupant's habits relating to sleep, room use, and time at home are intended to be shared with friends, strangers, commercial entities, the government or others.

3. Provide Incentives to Privatize Information—Revisit Consent

In this new informational age, there are few incentives to privatize information.[147] Commercial companies want as much

---

(July 30, 2010), http://www.wsj.com/articles/SB10001424052748703940904575395073512989404 (last visited May 4, 2015) (noting that Internet surveillance can even record an individual's favorite movies) (on file with the Washington and Lee Law Review).

143. *See id*. (explaining that codes have the ability to pinpoint an individual's behavior, including whether the user takes quizzes or browses entertainment websites).

144. *See id*. (specifying that companies use codes to combine a computer user's sex, age, and location with that user's internet activity).

145. *See, e.g.*, Adam Cohen, *Keeping Uncle Sam Out of Your Amazon Account*, TIME (Nov. 3, 2010), http://content.time.com/time/nation/article/0,8599,2029166,00.html (last visited May 4, 2015) (explaining that the federal courts denied North Carolina's request for individual consumer data for tax purposes because it violated the First Amendment and Video Protection Privacy Act) (on file with the Washington and Lee Law Review).

146. *See id*. ("[I]t would have a chilling effect on their decision about what to buy.").

147. *See* Jack M. Balkin, Essay, *The Constitution in the National Surveillance State*, 93 MINN. L. REV. 1, 16 (2008) (explaining that the government is increasingly turning to private companies to circumvent the Fourth Amendment).

information as possible for marketing and sales purposes and Web companies are happy to trade or sell information as a distinct market of its own.[148] Consumers often trust companies not to distribute information, but generally have no idea about what information is collected or distributed, and if it is distributed, to whom.[149] Privacy agreements generally serve as a barrier to customers, who must sign the agreements to access sites, not to the companies themselves.[150]

Another related issue is the "soft consent" required to use multifunctional devices.[151] Soft consent is the voluntary checking of a box that is taken as acknowledgement of reading, understanding, and agreeing with the privacy policy adopted by the online company.[152] Unfortunately, the agreeing does not require multiple sets of initials indicating that the important

---

148. *See* Angwin, *supra* note 142**Error! Bookmark not defined.** ("Consumer tracking is the foundation of an online advertising economy that racked up $23 billion in ad spending last year.").

149. *See* Viktor Koen, *Getting to Know You*, ECONOMIST (Sept. 13, 2014), http://www.economist.com/news/special-report/21615871-everything-people-do-online-avidly-followed-advertisers-and-third-party (last visited May 4, 2015) (providing anecdotal evidence that although many companies claim not to share sensitive personal and health information for advertising purposes, users who searched sexually transmitted diseases had advertisements about HIV support services days later) (on file with the Washington and Lee Law Review).

150. *See, e.g.*, *Customer Agreement*, AMAZON, http://aws.amazon.com/agreement/ (last visited May 4, 2015) ("This AWS Customer Agreement . . . contains the terms and conditions that govern your access to and use of the Service Offerings . . . .") (on file with the Washington and Lee Law Review).

151. Consent to spyware is not really consent at all because it piggybacks on the installation of another software program that the user actually wants. *See What is Spyware?*, MICROSOFT, http://www.microsoft.com/security/pc-security/spyware-whatis.aspx (last visited May 4, 2015) (on file with the Washington and Lee Law Review)

> A common trick is to covertly install the software during the installation of other software you want such as a music or video file sharing program . . . . Whenever you install something on your computer, make sure you carefully read all disclosures, including the license agreement and privacy statement. Sometimes the inclusion of unwanted software in a given software installation is documented, but it might appear at the end of a license agreement or privacy statement.

152. *See* Elizabeth Bowles & Eran Kahana, *The Agreement that Sparked a Storm*, 16 BUS. L.J. 55, 56 (2007) (explaining that click-wrap requires acceptance of the terms and conditions prior to accessing a website or installing software).

points have been read and understood, like many waivers or assurances of understanding.

The Fifth Amendment privilege against self-incrimination provides a useful analogue. Just as the *Miranda*[153] doctrine looked beneath the surface in determining whether the custodial interrogation environment created by police officers was coercive, courts should view the consent given by consumers in a similar manner—particularly with objectively sensitive information disclosed for a limited purpose, presumptively intended for a restricted disclosure unless shown to the contrary. The disclosure of information to a particular person for a specific reason should not always constitute consent to disclose that information to any outside parties not associated with the particular functionality of the device.

While many users of software willingly consent to turn over information, many do not know where the information goes or ends up.[154] Consent to endless disclosure without some understanding of the consequences and a means of providing more limited disclosure should not be considered fully voluntary.[155] Companies, such as Facebook, have long privacy policies with fine print, change their policies at will, and expect users to read license agreements and policies that have changed, regardless of background or age.[156] In the dominant culture, users must comply or be excluded—and perhaps lose a salient common social media connection with others.[157]

---

153. Miranda v. Arizona, 384 U.S. 436 (1966).

154. *See* Angwin, *supra* note 142 (describing several methods tracking devices use to get installed, some of which are unknown to most Internet users).

155. *See id*. (noting that sometimes tracking companies hide their data collection methods within other tracking files or advertisements).

156. *See* Drew Guarini, *Hold Your Gasp, Facebook is Under Fire for its Privacy Policy Again*, HUFFINGTON POST (Sept. 5, 2013), http://www.huffingtonpost.com/2013/09/05/facebook-privacy-ftc_n_3873764.html (highlighting the policy that states if the user is underage and agrees to the terms, it means "at least one of [the] parents or legal guardians have also agreed to the terms of the selection on the [child's] behalf," despite the fact that most parents are unaware of the privacy changes) (on file with the Washington and Lee Law Review).

157. *See* Laura Sydell, *Yet Another Shift in Facebook Policies Raises Privacy Concerns*, NPR (Nov. 29, 2012, 5:16 PM), http://www.npr.org/blogs/alltechconsidered/2012/11/29/166177278/yet-another-shift-in-facebook-policies-raises-privacy-concerns (last visited May 4, 2015) (including one businessman's remarks: "I know as a businessperson, everybody feels obliged to have a Facebook

The difference between physical consent in a face-to-face setting and an affirming keystroke can be significant. One need only look at the experience of intrusion occurring with brief traffic stops by the police, particularly DUI roadblocks,[158] to understand that the ease of a keystroke consent provides no real understanding of how Big Data algorithms will use information to combine it and search even the most intimate corners of a person's life—in seconds.

Thus, there should be legislation and renewed constitutional scrutiny about the scope of consent a website or device user gives to others as a consequence of such use. Password-protected or encrypted data indicates a greater interest in privacy, and forced education and even paternalism are justified when it pertains to data widely considered confidential in traditional American culture, such as medical, hygiene, and other intimate information that would adversely affect a person's reputation if disclosed publicly.[159]

4. Limit Bulk Collection of Data Unless Justified by Time, Place, and Circumstance

a. Require Particularity

While surveillance in the pre-digital age tended to be "retail," meaning targeted at individuals who were under suspicion of criminal behavior, the ease of data collection, storage, and analysis today have moved cybersurveillance to the "wholesale" realm.[160]

---

account. Ultimately it's a choice. But I really don't think that it is as much of a choice as it used to be . . . .") (on file with the Washington and Lee Law Review).

158. *See, e.g.*, Michigan v. Sitz, 496 U.S. 444, 447 (1990) (holding that Michigan's use of sobriety checkpoints did not violate the Fourth and Fourteenth Amendments).

159. *See* Dan Terizan, *The Fifth Amendment, Encryption, and the Forgotten State Interest*, 61 UCLA L. REV. DISC. 298, 298 (2014) (noting that encrypted devices are almost impenetrable).

160. *See* Gabriel Debenndetti, *Factbox: History of Mass Surveillance in the United States*, REUTERS (June 7, 2013, 4:48 PM), http://www.reuters.com/article/2013/06/07/us-usa-security-records-factbox-idUSBRE9 5617O20130607 (last visited May 4, 2015) (illustrating the major changes to government surveillance chronologically, starting in 1918 and concluding in 2013) (on file with the Washington and Lee law Review).

The interception of bulk phone records is but one illustration of how the government is now in the business of mass data gathering, sometimes irrespective of particular criminal justification.[161]

Today, it appears that much more information is recovered from non-targets than targets.[162] While that, in and of itself, is not necessarily problematic, if the analogue to the pre-digital world is applied, information obtained by inadvertent government spying, if not directly inculpatory, should be disposed of promptly—at the latest, after a reasonable length of time.[163] The case of *Warden v. Hayden*[164] is instructive. In *Warden*, police officers chased a fleeing felon into a house without a warrant.[165] In attempting to capture the felon, police searched the house. They found some incriminating clothes in the washing machine.[166] Prosecutors were allowed to use the clothes as evidence in the case at hand.[167] If the officers had searched a drawer, however, and obtained all of drawer's contents that did not relate to the case, the officers could not simply keep the contents indefinitely, waiting to see if that

161. *See, e.g.*, Mario Trujillo, *DEA Program Secretly Collected Bulk Phone Records for Decades*, THE HILL (Apr. 7, 2015, 6:03 PM), http://thehill.com/policy/tech nology/238135-dea-program-collected-bulk-records-on-americans-international-calls (last visited May 4, 2015) (describing the DEA's now defunct bulk phone-record data collection program) (on file with the Washington and Lee Law Review).

162. *See* Barton Gellman, Julie Tate & Ashkan Soltani, *In NSA-intercepted Data, Those Not Targeted Far Outnumber the Foreigners Who Are*, WASH. POST (July 5, 2014), http://www.washingtonpost.com/world/national-security/in-nsa-intercepted-data-those-not-targeted-far-outnumber-the-foreigners-who-are/ 2014/07/05/ 8139adf8-045a-11e4-8572-4b1b969b6322_story.html (last visited May 4, 2015) (describing the bulk collection of data as premised on finding a legal or criminal issue from the data, not on an issue that already exists prior to collection) (on file with the Washington and Lee Law Review).

163. *But see* Trujillo, *supra* note 161 (noting that a government data-collection program only ended after Edward Snowden's surveillance information leak).

164. 387 U.S. 294 (1967).

165. *See id*. at 297 (recounting that the police entered a house without a warrant after believing a robbery suspect was hiding inside).

166. *See id*. at 298 (chronicling that the police searched the entire house, including the bathroom after noticing the sound of running water).

167. *See id*. at 309 (rejecting the mere evidence rule).

information would become relevant to a current or future case.[168] That is what bulk collection involves.[169]

b. Keep the Warrant Requirement as the General Rule

When Google bought the company Nest, the company that makes the "learning thermostat," Nest issued a statement reassuring customers that its privacy policy "clearly limits the use of customer information to providing and improving Nest's products and services. We've always taken privacy seriously and this will not change."[170] Of course, taking privacy seriously and acting as a privacy advocate are not necessarily the same. Customer information could still be used in an anonymized fashion[171] and then traded or sold.[172]

With the public/private and investigative/gathering lines blurring in the digital age, lines drawn to indicate how far government can go in collecting, sorting, and analyzing data are more important than ever before. Newly developed technologies are allowing the government to overreach into the private sphere.[173] That is why warrants are especially important today, not only to prevent overreaching in specific cases, but to deter

---

168. *See id*. at 307 ("Thus in the case of 'mere evidence,' probable cause must be examined in terms of cause to believe that the evidence sought will aid in a particular apprehension or conviction.").

169. *See White House Allows NSA's Bulk Data Collection to Continue*, CBS NEWS (Feb. 3, 2015, 5:23 PM), http://www.cbsnews.com/news/white-house-allows-nsa-bulk-data-collection-to-continue/ (last visited May 5, 2014) (highlighting that the new limits on governmental bulk data collection are so broad that they do not serve as a real check on the NSA) (on file with the Washington and Lee Law Review).

170. *See* Matt Rogers, *Nest, Google and You*, NEST (Jan. 13, 2014), https://nest.com/blog/2014/01/13/nest-google-and-you/ (last visited May 5, 2014) (issuing a release about the effect of the buyout on customers) (on file with the Washington and Lee Law Review).

171. *Id*.

172. *Id*.

173. *See* Oren Bar-Gill & Barry Friedman, *Taking Warrants Seriously*, 106 NW. U. L. REV. 1609, 1621 (2012) (noting that bright-line rules might simplify matters but are likely to hurt law enforcement as well).

overreaching as well.[174] In *United States. v. Warshak*,[175] the Sixth Circuit held that there was sufficient privacy in the content of emails for the police to need a warrant to obtain them.[176] The Court noted that there was considerable information in the defendant's thousands of emails obtained by the police, yielding a treasure trove of information.[177] This case provided important recognition that warrants are still required for most criminal government investigations.

As technology advances, it will become easier and easier for police to obtain direct access to information without a warrant.[178] That does not mean the shortest path is the proper one.[179] One illustration of the new technology is the Range-R, a device that operates like a wall-stud finder, but permits an operator on the outside of a residence or building to detect whether someone is present in the home and where that person is located.[180] In effect, it operates like a motion detector from outside the residence, and has been used by police domestically before entering the home of private individuals.[181] Physical walls simply are less viable as a constitutional privacy boundary as time marches on.

---

174. *See* William J. Stuntz, *Warrants and Fourth Amendment Remedies*, 77 VA. L. REV. 881, 918 (1991) (explaining that warrants have a deterrent effect due to the evidentiary exclusionary rule).

175. 631 F.3d 266 (2010).

176. *See id*. at 284 (explaining that it is highly unlikely that people expect their emails containing business and personal matters to be made public because "people seldom unfurl their dirty laundry in plain view").

177. *See id*. at 288 (emphasizing the "potential[ly] unlimited variety of 'confidential communications'" in the *Katz* Court's analysis).

178. *See* Daniel Zwerdling, *Your Digital Trail: Does the Fourth Amendment Protect Us?*, NPR (Oct. 2, 2013, 1:00 PM), http://www.npr.org/blogs/alltechconsidered/2013/10/02/228134269/your-digital-trail-does-the-fourth-amendment-protect-us (last visited May 6, 2015) (explaining that instead of a warrant, law enforcement can just obtain a subpoena) (on file with the Washington and Lee Law Review).

179. *See id*. (using the cloud as an example of how the government can get around the warrant requirement).

180. *See* Laura Sullivan, *New Tools Let Police See Inside Peoples' Homes*, NPR (Jan. 21, 2015, 10:18 PM), http://www.npr.org/blogs/thetwo-way/2015/01/21/378851217/new-tools-let-police-see-inside-peoples-homes (last visited May 6, 2015) (noting that the use of the Range-R has been questioned by an appellate court in Denver) (on file with the Washington and Lee Law Review).

181. *See id*. (reporting that the Justice Department refused to say how often the Range-R is utilized).

5. Keep Score—Legislate How Private Companies Are Doing with Our Privacy, Especially with Government Sharing

A different way to reign in the government is through the private companies who partner and share information with government entities. As noted above, there is little incentive for companies to privatize information that could be used for marketing purposes or valued as a commodity.[182] Without independent consumer action, legislation offers a way to cabin greed and protect consumers.[183] Much like ingredients posted on food packages, there should be legislative requirements to create notice about how private companies deal with privacy issues.[184] This transparency will help assuage misunderstandings, promote a more informed public, and allow for discourse, even pressure, about company practices.[185]

Currently, the watchdog group Electronic Frontier Foundation (EFF) compares how private companies stack up in their potential partnering with the government through different types of measurables.[186] These measurables, published in a report by EFF titled, "Protecting your Data from Government Requests," include: requiring a warrant for content, informing users about government data request, publishing transparency reports for consumers, publishing law enforcement guidelines, advocating for users' privacy rights in courts, and fighting for users' privacy rights in Congress.[187]

---

182. *See* Balkin, *supra* note 147 (explaining the benefits of privatization).

183. *See* Robert Rampton & Alina Selyukh, *Obama Proposes New Data Laws as U.S. Central Command Hacked*, REUTERS (Jan. 12, 2015, 2:33 PM), http://www.reuters.com/article/2015/01/12/us-usa-obama-cybersecurity-idUSKBN0KL0EI20150112 (last visited May 6, 2015) (underscoring the importance of consumer protection as data breaches become more prevalent) (on file with the Washington and Lee Law Review).

184. *See id*. (providing one example of proposed legislation requiring companies to inform consumers within thirty days of the discovery of a breach that their information was compromised).

185. *See id*. (extolling the benefits of proposed legislation that would keep consumers informed about how companies mine data on individual consumers).

186. *See Who Has Your Back? Protecting Your Data from Government Requests*, ELECTRONIC FRONTIER FOUND., https://www.eff.org/who-has-your-back-2014 (last visited May 6, 2015) (providing a review of major companies based on their privacy policies) (on file with the Washington and Lee Law Review).

187. *See id*. (explaining the results in an easy-to-understand chart).

6. Maintain Constitutional Accountability of the Military—Revitalize the Third Amendment's Role by Limiting Cyber Soldiers in and Around Civilian Life

> "No soldier shall, in time of peace, be quartered in any house, without the consent of the Owner, nor in time of war, but in a manner to be described by law."[188]

While wars are still being fought out on battlefields today, state-sponsored hackers on the Internet are also fighting them.[189] The Department of Defense has its own battalion of cyber soldiers.[190] These cyber soldiers know no boundaries, seeking enemies within and around civilian locations as well as clear army bases and fields of war.[191]

Although the Fourth Amendment has been used in modern times as the sole source of search and seizure limitations, the Third Amendment should be added to the privacy calculus.[192] The Third Amendment provides a clear allocation of power between military and civil authorities and creates a realm of privacy governed by civil law.[193]

The forgotten Third Amendment, though slumbering in desuetude, does have relevance today.[194] The Amendment, at a

---

188. U.S. CONST. amend. III.

189. *See* Michael A. Riley & Jordan Robertson, *Chinese State-Sponsored Hackers Suspected in Anthem Attack*, BLOOMBERG (Feb. 5, 2015, 2:42 PM), http://www.bloomberg.com/news/articles/2015-02-05/signs-of-china-sponsored-hackers-seen-in-anthem-attack (last visited May 6, 2015) (reporting that Chinese state-sponsored hackers attacked Blue Cross Blue Shield causing a security breach) (on file with the Washington and Lee Law Review).

190. *See Army Cyber*, U.S. ARMY CYBER COMMAND, http://www.arcyber.army.mil (last visited May 6, 2015) (providing information on United States cyber soldiers) (on file with the Washington and Lee Law Review).

191. *See id.* ("USCYBERCOM plans . . . activities to: direct the operations and defense of . . . information networks and; prepare to . . . conduct full-spectrum military cyberspace operations . . . to enable actions in all domains, ensure US/Allied freedom of action in cyberspace and deny the same to our adversaries.").

192. *See* Geoffrey M. Wyatt, *The Third Amendment in the Twenty-First Century: Military Recruiting on Private Campuses*, 40 NEW ENG. L. REV. 113, 122–24 (2005) (explaining the dual rationales of the Amendment).

193. *See* Tom W. Bell, *The Third Amendment: Forgotten But Not Gone*, 2 WM. & MARY BILL RTS. J. 117, 141 (1993) (describing the Third Amendment's role in privacy doctrine).

194. *See id.* at 117 (lamenting that the Third Amendment receives little legal or academic attention).

minimum, helps to ensure dividing lines between the civilian and military worlds.[195] In the 18th century, the physical quartering of soldiers in civilian homes epitomized this dividing line.[196] Today, the physical quartering is not as significant as the cyber soldiers who hack into computers, track cell phones, use high-flying drones, face-recognition software, and private-company data to obtain information about our private lives—without any discrimination between what happens inside the home or outside.[197] Given that the military presence can be just as intrusive even if not seen or experienced, the Amendment's check on government tyranny should be viewed as restricting cyber soldiers from focusing surveillance instrumentalities on and around private residences or businesses in an intrusive way—or using proxies to do so—that would serve as the functional equivalent of military quartering in the civil community.[198] While the government can of course track and prevent terrorist activities if possible, that objective differs from mass surveillance of citizens without any reasonable justification.

If the Third Amendment is not read as surplusage, it will help differentiate between government agencies storing and using the data of everyday citizens, and provide at least another check in recognizing that military action often differs from crime interdiction by local, state, and federal law enforcement.[199] Invisible federal cybersurveillance of our residences and

---

195. *See* United States v. Walden, 490 F.2d 372, 375 (4th Cir. 1974) (demonstrating the limited role in the civilian sphere).

196. *See* Bell, *supra* note 193, at 125 ("The Third Amendment was directly inspired by the abuses colonialists suffered at the hands of British soldiers immediately prior to and during the Revolutionary War.").

197. *See* Thomas L. Avery, *The Third Amendment: The Critical Protections of a Forgotten Amendment*, 53 WASHBURN L.J. 179, 205 (2014) (claiming that the Third Amendment needs to be interpreted more broadly to protect citizens from modern-day quartering involving technological advances).

198. Instrumentalities do not include malware such as the "Stuxnet" computer worm, tracking devices, cookies, and more. The Stuxnet worm was allegedly used by several countries to infiltrate and infect Iran's nuclear facilities. *See* Alan Butler, *When Cyberweapons End Up on Private Networks: Third Amendment Implications for Cybersecurity Policy*, 62 AM. U. L. REV. 1203, 1204–05 (2013) (discussing cybersurveillance on private networks).

199. *See* Avery, *supra* note 197, at 198 (arguing that there are fewer protections regarding military surveillance via the Third Amendment than there are police surveillance via the Fifth Amendment).

communities should not be permitted to usurp the state and local crime interdiction based on a vague reference to terrorism.[200]

IV. Conclusion

The development of the Internet of Things, involving interconnected multifunctional devices that can "learn" as they spy on us, has numerous implications for self-cybersurveillance issues.[201] In a very real sense, the Internet of Things creates self-mass surveillance systems, many of which will eventually lead to feeding data to the government, either directly or through partnerships between the government and private industry.[202] As 20th century notions of privacy recede and become antiquated, the Third and especially Fourth Amendments, as well as the separation of powers, must be implicated in order to preserve the value of privacy and keep it from slipping closer to extinction.[203] The brick and mortar cases from a bygone era, especially *Smith v. Maryland* and *United States v. Miller*, have an all-or-nothing quality that do not provide helpful guidance or realistic analysis for the present day.[204] Instead, courts should adopt a Fourth Amendment theory that maintains government accountability and minimizes the gathering and use of incidental information by the government.[205]

In this age of complexity and uncertainty, however, the Constitution alone will not protect privacy.[206] Legislation should be enacted to incentivize the public/private distinction and maintain information as private. Further, legislation should promote transparency about what companies are doing with the

---

200. *See id.* at 199 (explaining that the military can circumvent the Third Amendment due to its plain-word interpretation).

201. *See supra* Part I (describing the Internet of Things).

202. *See id.* (highlighting the problematic consequences to consumers).

203. *See* Avery, *supra* note 197, at 198 (claiming that the Third Amendment needs a *Miranda* moment).

204. *See supra* Part III (discussing *Smith v. Maryland* and its consequence on the expectation of privacy).

205. *See supra* Part III (proposing judicial safeguards to combat the diminishing privacy right as technology increases).

206. *See* Rampton & Alina *supra* note 183 (providing safeguards protecting consumers).

information they collect.[207] Transparency can occur by requiring companies to create the equivalent of food labels—having private companies publicize their relationship with the government—to inform consumers about what types of information are or might be shared.[208] In addition, there should be well-defined limits on government access to self-cybersurveillance information and stronger consent requirements for sharing such information with third parties.[209] The right to privacy is too important to be allowed to disintegrate before our eyes.

****

207. *See id*. (claiming that legislation was proposed to combat these issues).
208. *See supra* Part III (describing the food-safety comparison safeguard).
209. *See supra* Part III (noting additional safeguards).