Drinking from the Fire Hose: How Massive Self-Surveillance from the Internet of Things is Changing the Face of Privacy

Steven I. Friedland
Elon University School of Law

Follow this and additional works at: https://researchrepository.wvu.edu/wvlr

Part of the Constitutional Law Commons, Fourth Amendment Commons, Privacy Law Commons, and the Science and Technology Law Commons

Recommended Citation
Available at: https://researchrepository.wvu.edu/wvlr/vol119/iss3/5
DRINKING FROM THE FIRE HOSE: HOW MASSIVE SELF-SURVEILLANCE FROM THE INTERNET OF THINGS IS CHANGING THE FACE OF PRIVACY

Steven I. Friedland*

ABSTRACT.................................................................................................................. 891
I. INTRODUCTION.................................................................................................... 892
II. THE INTERNET OF THINGS............................................................................... 894
III. THE NEW SELF-CYBERSURVEILLANCE AND THE IoT.......................... 897
IV. HOW THE SELF-CYBERSURVEILLANCE OF THE IoT HAS LOOSENED THE MOORINGS OF PHYSICAL WORLD PRIVACY ........................................... 898
   A. Start with the Internet's Business Foundation—Surveillance........................ 898
   B. The Pervasiveness and Insecurity of the IoT............................................ 900
      1. Pervasiveness ......................................................................................... 900
      2. Insecurity .................................................................................................. 903
         i. Multiple Weaknesses ......................................................................... 905
         ii. “Always On” Devices......................................................................... 905
V. SAFEGUARDING PRIVACY IN AN IoT WORLD ................................................. 906
   A. The Fourth Amendment as a Protective Source ........................................ 907
   B. A Culture of Vigilance ................................................................................ 911
   C. Company-Consumer Alliances .................................................................. 912
VI. CONCLUSION .................................................................................................... 912

ABSTRACT

In an era of diminishing privacy, the Internet of Things ("IoT") has become a consensual and inadvertent tool that undermines privacy protection. The IoT, really systems of networks connected to each other by the Internet or other radio-type device, creates consensual mass self-surveillance in such domains as fitness and the Fitbit, health care and heart monitors, "smart" houses

* Steven I. Friedland is the Associate Dean for Innovations in Engaged Learning in Law and Professor of Law and Senior Scholar at Elon University School of Law. He would like to thank his most capable research assistants, Ragan Riddle, Candace Washington, Paige VanKooten, and Talia Nowicki for their excellent work and the Elon Law Librarian, Lisa Watson, for her ready assistance.
and cars, and even "smart" cities. The multiple networks also have created a degree of interconnectivity that has opened up a fire hose of information for companies and governments alike, as well as making it virtually insuperable to live "off the grid" in the modern era. This treasure trove of information allows for government tracking in unprecedented ways. This Article explores the influence of the IoT, the mass self-surveillance it produces on privacy, and the new shapes of privacy that are emerging as a result. This Article offers several forms of protection against the further dissipation of privacy.

We have met the enemy, and he is us.
—Theunis Bates

I. INTRODUCTION

We live in a world of diminishing privacy. Walls and doors once protected our personal secrets from governments as well as nosy neighbors. Today, our hyper cyber-connected life has created ocean-sized data flows, a potent information marketplace, and public revelation of personal and even intimate secrets, some usually reserved in the past only for individual diaries or discussions behind closed doors. If a person lives "on the grid," her intimate and valued information sooner or later likely will be subject to access to third parties—and possibly to the eventual sale or distribution of that information to others far downstream of its intended disclosure. Significantly, big chunks of this information can end up in government hands, to be stored indefinitely and used without oversight. Governments are collaborating with companies, other countries, and individuals to obtain information, in addition to accessing information about individuals directly.

The rise of self-cybersurveillance, meaning the intentional or consensual creation of mass information about oneself through electronic tracking or other means, has not only changed daily life for millions of individuals, but also the nature of personal privacy. One significant stimulus promoting massive data creation, collection, and transfer is what has been loosely described as the IoT. The IoT, more aptly described as an aggregation of systems of networks connected to each other by the Internet or other radio-type device, creates consensual mass self-surveillance in such domains as fitness and the Fitbit.

2 See Niva Elkin-Koren & Eldar Haber, Governance by Proxy: Cyber Challenges to Civil Liberties, 82 BROOK. L. REV. 105 (2016).
health care and heart monitors, "smart" houses\(^5\) and cars, and even "smart" cities.\(^6\) The IoT networks are really an outgrowth of the development of pervasive computing, which has blurred the boundaries of the digital and physical worlds. These networks have created a degree of interconnectivity that has opened up a fire hose of information for individuals, companies, and governments, as well as made it virtually insuperable to live "off the grid" within society.\(^7\) This treasure trove of information allows for government tracking in unprecedented ways.

This Article explores the influence of the IoT on privacy, particularly the mass self-surveillance it produces and the new shapes of privacy that are emerging as a result. The impact on privacy has been profound, leading privacy to become a shapeshifter, or transmogrified, especially under the Fourth Amendment and its protection of that which falls within a "reasonable expectation of privacy."\(^8\) To protect against the uncontrolled transmogrification of privacy in the future, safeguards must be made that are structural and not merely ad hoc.

Different steps can be taken to enhance privacy safeguards, many of which are interrelated.\(^9\) One step involves constitutional interpretation. The Fourth Amendment ought to be interpreted to recognize the prevalence and importance of limited purpose disclosures, much like the idea of privileges used to promote certain relationships. Another step is rooted in contracts and property law. The disclosure of information gathered by websites and other IoT devices cannot simply be based on a clicked consent, but rather as a license to allow a digitized component of physical property to be shared with a manufacturer or specified third parties. In this way, the IoT should not be allowed to create free information as a by-product of its structure, but rather implicit licenses of information.

Yet another step involves stronger cultural privacy norms. If the legal limitations of disclosure continue, norms must arise that encourage citizens to be more vigilant about the nature and types of information voluntarily distributed to others.

---


9 See Anita L. Allen, Protecting One's Own Privacy in a Big Data Economy, 130 HARV. L. REV. FORUM 71 (2016).
A different step puts pressure on commercial enterprises through the doctrine of interest convergence. This doctrine claims that outcomes often depend on an alignment of interests that overcomes significant difference in individuals or groups. One illustration of this occurred in the 2015 Apple-U.S. Government stand-off, when Apple refused to provide government access to the locked cell phone of an American terrorist possibility because of how consumers and other governments would react if they did. In addition, greater use of encryption, despite the potential of “going dark,” can readily promote individual privacy interests.

Even if these changes suffice, government regulation will still be needed to ensure a modicum of transparency about the scope of government programs, including how and when companies are cooperating with the government in providing information. This assurance of transparency is necessary to ensure that checks and balances are in place consonant with democracy.

II. THE INTERNET OF THINGS

The ... first 20-odd years of the web have been focused on human beings. The next era is going to be inanimate things.

—Julianna Pepitone

The IoT is larger and more organic in actuality than just things connected to the Internet. While a central IoT component consists of a group of devices connected to the Internet through local Internet Protocol (“IP”) addresses, that conceptualization does not accurately portray its true scope. The IoT is more properly described as groups of devices connected to networks for a particular reason. While some IoT networks link to the Internet, not all do—or need to do so—to function within their domains. Furthermore, wherever a sensor can be embedded to first collect and then transmit data, the IoT can be found—even if


14 These addresses are composed of 32 bytes expressed as four groups of numbers separated by periods. For example, 356.202.413.100 might be one IP address.

the device is not measuring a thing, but rather an intangible, like the wind, temperature or how well someone is sleeping.

The use of embedded sensors in networks is proliferating, with a billion connected devices expected by the year 2020. In fact, the growth of the IoT is occurring at a "dangerously fast pace," leading to estimates of more than 40 billion devices by the year 2020.

A common thread in the IoT firmament is the presence of semi-autonomous data-generating sensors. The radio-transmitting sensors in the devices generally monitor things with a specific purpose. For example, a smart thermostat monitors temperature, but it learns to do so at a time when the temperature really matters, such as when the residents of the home or office are present. A car might have special sensors for its backup camera so the camera can photograph relevant areas around the car when it is moving, especially in reverse, and a radar system to determine what objects are nearby. These features are automated to a large extent, allowing some devices to operate remotely.

The sensors are connected to each other by tiny radio transmitters that form the backbone of IoT networks. These networks, like subway systems, include the Internet and Local Area Networks (“LAN”). Often, the transmitter will connect through Wireless Fidelity (what is commonly called “Wi-Fi”), but can communicate through less powerful connections such as Bluetooth transmission.

A key to understanding the devices within the IoT is that they are generally multifunctional, such that their form and function can be separated. In other words, they are physical devices with a separate digital function. A smart watch, for example, offers the time, but also might provide the temperature and email. A smart car transports its occupants, but also can have systems that collect and transmit data for specific functions, such as automated backup.

---


17 Id.

18 Id.


22 These networks use special ways to communicate. The most common one today is the Transmission Control Protocol/Internet Protocol (“TCP/IP”).

cameras, radar detection, and brake sensors. The smart television set not only provides programming, but can be triggered remotely by commands from voice activation.

Conceptualizing the IoT as one contiguous whole also misses the specific functional purposes of the networks. The nature and scope of the connected devices often depend on a particular industry or commercial domain within which the devices operate. In essence, the devices are purposed within the context of the setting and are automated or set to collect and transmit data for a specific reason. That is why there are different types of interconnectivity within the home (such as for appliances and lights), cars (such as for location and brakes), clothing (such as for location and condition), medicine (for heart rate and exercise), unmanned aircraft (drones), armaments (weaponry, such as planes), businesses, and even cities (for electric grids and security). That is also why the description, “Internet of Everything,” misses the import of the domain-specific significance of IoT spheres.

In effect, the term “Internet of Things” is a proxy for a conceptualization of the way devices can communicate and connect with each other to accumulate,

---


25 See, e.g., Not In Front of the Telly: Warning Over “Listening” TV, BBC NEWS (Feb. 9, 2015), http://www.bbc.com/news/technology-31296188. As stated in the article:

The policy explains that the TV set will be listening to people in the same room to try to spot when commands or queries are issued via the remote. It goes on to say: “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.

sort, and transmit data.\textsuperscript{27} Perhaps the most that can be said about pinning down an exacting scope of the IoT is that its definition is evolving.\textsuperscript{28}

III. The New Self-Cybersurveillance and the IoT

Perhaps the overriding consequence of the IoT’s interconnecting devices is to create multiple systems of not just mass surveillance, but massive surveillance. These self-surveillance systems have different levels of breadth and depth—some systems are micro-based, such as how active a person is who wears a cyberonic device like a FitBit, and some are macro-based, such as monitoring an area of a city for electricity consumption, traffic patterns, and criminal activity.\textsuperscript{29} The micro-oriented surveillance often becomes a component of larger systems. The heart-tracker, for example, joins with a blood pressure evaluation, a sleep assessor, and a step measurer\textsuperscript{30} to create a better gage of personal health. A single individual’s information, in turn, can be accessed, aggregated—even anonymized—and sorted by health companies or insurers to predict health trends and create more efficiencies in their businesses.

The information generated by the transmitting devices can be readily shared with application developers, manufacturers, and other interested third parties.\textsuperscript{31} The commodification of such information has been occurring without much regulation for more than a decade. Significantly, the data trail often is invisible. Unlike a police tail or cameras fixed on buildings, even the surveillance from the interconnected devices lies submerged and generally does not create the experience of intrusion or intervention. The data transmission may cause little

\textsuperscript{27} See, e.g., Jacob Morgan, \textit{A Simple Explanation of “The Internet of Things”}, FORBES (May 13, 2014, 12:05 AM), http://www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand/#605a9f096828. Morgan stated:

Simply put, this is the concept of basically connecting any device with an on and off switch to the Internet (and/or to each other). This includes everything from cellphones, coffee makers, washing machines, headphones, lamps, wearable devices and almost anything else you can think of. This also applies to components of machines, for example a jet engine of an airplane or the drill of an oil rig.

\textit{Id.}


\textsuperscript{31} Most manufacturers will be able to share user information.
fear precisely because the potential harms from shared information are unseen and often surface far downstream.\textsuperscript{32}

Another salient feature of the IoT surveillance systems is that they are generally voluntary, initiated with the express or implicit consent of the surveilled. That is, the subjects either initiate surveillance (e.g., put on wearable tech or buy a smart television) or consent to surveillance (e.g., html cookies deposited in websites). The information starts flowing by being consensually shared with the application maker or software manufacturer, and then often finds its way into the broader information marketplace. The information stream can then move readily from within the industry domain to the government.

While this flow of information is often understated or hidden, that is not always the case. Sometimes, the notice of data collection and transfer is clearly asserted. One example is the website thenextweb.com ("TNW").\textsuperscript{33} Prominently featured on the Web page is a video vine of a person eating a real cookie, with the statement underneath: "TNW uses cookies to personalize content and ads to make our site easier for you to use. We do also share that information with third parties for advertising and analytics."\textsuperscript{34} While this pronouncement likely does not deter users from accessing the site, it does show that the information stream goes to unknown sources.

IV. HOW THE SELF-CYBERSURVEILLANCE OF THE IoT HAS LOOSENED THE MOORINGS OF PHYSICAL WORLD PRIVACY

A. Start with the Internet’s Business Foundation—Surveillance

Several important complicating factors have hastened the shapeshifting of privacy. One significant precursor to the IoT was the business model that evolved to commoditize the Internet. Instead of being premised on a system of pay for use, the Internet monetized advertising. It was not just ads that were the cornerstone of the economic structure, but by making users the product, it focused on the surveillance of the users. In essence, surveillance was the key to the profitability of the World Wide Web. Ethan Zimmerman, one of the creators of the "pop-up" advertisement on the web, has written an insightful reflection of where good intentions to develop the web in a certain way may have gone awry:


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 IoT.


\textsuperscript{34} Id.
I have come to believe that advertising is the original sin of the web. The fallen state of our Internet is a direct, if unintentional, consequence of choosing advertising as the default model to support online content and services. Through successive rounds of innovation . . . we’ve trained Internet users to expect that everything they say and do online will be aggregated into profiles (which they cannot review, challenge, or change) that shape both what ads and what content they see. Outrage over experimental manipulation of these profiles by social networks and dating companies has led to heated debates amongst the technologically savvy, but hasn’t shrunk the user bases of these services, as users now accept that this sort of manipulation is an integral part of the online experience.

Users have been so well trained to expect surveillance that even when widespread, clandestine government surveillance was revealed by a whistleblower, there has been little organized, public demand for reform and change. . . . It’s unlikely that our willingness to accept online surveillance reflects our trust in the American government . . . More likely, we’ve been taught that this is simply how the Internet works: If we open ourselves to ever-increasing surveillance—whether from corporations or governments—the tools and content we want will remain free of cost.35

What Mr. Zimmerman is effectively observing is that the reasonable expectations of online users now include manipulation and tracking. If this notion of expectations shaped by culture and technology prevails, privacy will exist only in fractional parts, becoming part social choice—whether to participate in common social groups, such as Facebook and Instagram—and whether to find alternative, more secure methods of communication, such as Signal36 or WhatsApp.37

B. The Pervasiveness and Insecurity of the IoT

1. Pervasiveness

The idea of pervasive computing, where the digital invades the physical world, has become a reality with the IoT. The result is a transformative experience, as well as a surfeit of data. The amount of data that can be generated by the IoT is voluminous, even by digital era standards. A Federal Trade Commission report found that fewer than 10,000 homes can generate up to 150 million data points per day. With such loads of information generated every day, entry points for hackers and third parties in general are exponential in number.

It is not just the volume of the IoT data that can make users wary. Information generated by self-surveillance can be permissibly accessed in ways unimaginable just decades ago. While often unseen, the new systems are firmly entrenched in a rapidly changing world. Within the new systems are various access points that are accessible by consent—or in the current culture of technology, hacking. As one commentator noted:

We let Facebook and Google scour our private messages, photos and search queries so they can better tailor advertising to us. Our GPS-enabled smartphones allow Apple and other companies to track our location and movements. And now millions of people are installing always-listening smart speakers in their homes... In theory, smart speakers record only those commands [directed to them], and everything else they hear is deleted. But hackers have already cracked into Wi-Fi baby monitors and it seems inevitable that an enterprising cybercriminal... will figure out how to eavesdrop through these gadgets.

39 Id.
42 Bates, supra note 1.
The prevalence of surveillance, particularly when contrasted with security interests, can be illustrated by developments in each wave of technology. Three such examples in the current wave are the “Beware” program by Intrado, Clear Channel Outdoor’s smart billboards, and smart athletic shirts.

Intrado, a subsidiary of the West Corporation, manufactures proprietary commercial software called Beware, which assigns “threat scores” to local residents. While the information utilized is not all from the IoT, much of it is self-created by voluntary actions available to the public. According to the company’s website:

Beware uses a patent-pending, web-search algorithm to scan massive amounts of commercial data and presents it as actionable intelligence, complete with threat scores in an easy-to-read headline format—all within seconds of an initial query.

The scores created by the software are red, yellow, or green, depending on the algorithm’s conclusions. The software sifts information from commercial data brokers that include publicly available records—arrests and conviction records, health history, property and commercial databases, and social media postings. The software can sort billions of data points in seconds. The tool currently is being used by the Fresno, California, Police Department, with more departments likely to follow if the program is successful. According to the company that makes the software, “Beware is a tool built to help public safety agencies inform first responders about the environment they may encounter when responding to a 9-1-1 call.”

The Beware program illustrates the importance of information transparency to privacy and provides ample evidence of the problems attendant to surveillance without oversight or checks and balances. The use of propensity-

---


45 Id.


47 Tan, supra note 44.

48 Id.

49 Id.
based analysis triggers many salient questions. What ingredients or information are used in the Beware algorithm—such as from social media posts and other public sources? How much came from the IoT, and how is it weighted? Does old information get discounted or discarded? Is the threat score contextualized to the situation and others who might be at the scene of a 911 call? If the formula is a trade secret, as claimed, how does anyone know if it is discriminatory or simply another form of profiling? Also, when and how often does a rigorous review of the accuracy and reliability of the algorithm’s scientific theory occur?

These and other questions will persist, especially as such programs continue to operate in secret, while propensity to behave in certain ways becomes an increasingly marketable commodity. The questions show that propensity analysis often might disrupt settled expectations of privacy. The issues with Beware also show that the disclosure of information is not about the first receiver of it, but where it might end up—in a program such as Beware and the government, or in many other locations. Another significant illustration of propensity-based tracking based on self-produced information involves the largest supplier of outdoor billboards, Clear Channel Outdoor.50 The company has announced the creation of smart billboards, using a program called Radar.51 These billboards can track the cell phones possessed by drivers and passengers in the vicinity of the billboards, and then follow-up and determine whether these individuals have accessed the website of the company whose ad the billboard was advertising. While not exactly parallel to the film Minority Report,52 in which a small poster ad specifically targeted the protagonist, John Anderton, to sell him a particular type of beverage, it does create a whole new form of performance tracking.

Smart athletic shirts provide another illustration of how the IoT will cause further shapeshifting of privacy.53 Over the past several decades, college sports departments have entered deals with apparel companies for millions of

52 MINORITY REPORT (Cruise/Wagner Productions 2002).
53 This dilemma will arise at all levels of sport. Major League Baseball, for example, approved wearable technology during games in 2016. Mike Vorkunov, Innovation vs. Invasion of Privacy: MLB Wearable Technology Battle Looms, USA TODAY (Sept. 22, 2016, 12:48 AM), http://www.usatoday.com/story/sports/mlb/2016/09/21/innovation-vs-invasion-privacy-mlb-wearable-technology-battle-loom/90783188/. Players can wear the Zephyr Bioharness to track their breathing and heart rate, as well as the Motus Sleeve, which has a chip in it that tracks arm angles and the forces placed on the ligaments in the elbow from throwing. Id.
In recent years, these deals have taken on a transformative dimension, providing that the players will be given smart apparel that contains tiny radio sensors allowing for the collection, transmission, and evaluation of biometric data. The transfer of such data raises the question of who owns the information produced. As one commentator noted, wearable technology might be the next frontier for athletes' rights in big-time college sports. At the University of Michigan, for example, a school that has a contract for wearable technology, this issue is already emerging. The wearable clothing incorporates different sensors that can collect an array of data, such as data related to speed, distance, vertical leap, height, maximum time aloft, shot attempts, length of ball possession, heart rate, and running routes.

When student-athletes wearing smart apparel start transmitting data to third parties, a significant question arises as to whether the young athletes will have any security or privacy protections in their information. Once the information is released, it will be next to impossible to return it to a "forgotten" status. While the contract at the University of Michigan apparently states that the data collection will be anonymous and comply with all of the applicable laws, it would not be difficult to de-anonymize the data, hack it, or both. The dilemma of who owns self-generated information is an especially thorny one in this context and is not readily resolved by existing legal structures. These questions implicate the pliability and varying contexts of consent, and how important the definition and application of the rule are to IoT issues. Without greater regulation, understanding, and attention paid to the issue, the greater our acquiescence to tracking by third parties will be.

2. Insecurity

Insecurity of the IoT is a significant impediment to the benefits it offers. The problems are both perceived and real. One study showed that 44% of the people polled were "very concerned" that their information would be stolen. In actuality, researchers have demonstrated the ability to hack into many IoT devices, from stopping cars remotely while they are driven on a highway, to Samsung's SmartThings smart home platform.

---

55 See Tracy, supra note 54.
56 Id.
57 Meola, supra note 41.
58 Id.
It is not simply uninvited access by hackers who can take down an entire power grid. The government partners with companies to get access to the company’s information, as what occurred with Yahoo and the United States government in 2015. There are also requests for permission to access information by companies through long and detailed consent agreements that often are not read by consumers, or government requests of companies to disclose. For example, a man was accused of killing a friend in Arkansas in 2016, and state police subpoenaed the only “eyewitness” to the crime—the interactive Amazon Echo automated “personal assistant,” located in the same room, that was possibly listening to the incident. The Echo is a free-standing electronic device that connects to a network through Wi-Fi and can be asked all sorts of questions—about the weather, news, etc.—or tasked with keeping grocery and other lists. The Echo “listens” for the special word that activates it for commands. As one journalist asked about the situation, “Namely, is there a difference in the reasonable expectation of privacy one should have when dealing with a device that is ‘always on’ in one’s own home?” Amazon, like Apple before it, is refusing to turn over to the police the data it has from the device, claiming customer privacy as the reason. Yet, other IoT information also might be pertinent. The government investigators have learned from a smart water meter on the premises that “an increase in water use in the middle of the night suggests a possible cleanup around the crime scene.”

59 Id.
63 Wang, supra note 61.
64 Id.
65 Id.; see also Tsukayama, supra note 43.
i. Multiple Weaknesses

A significant problem with IoT sensor networks is the multiple inflection points that are vulnerable to hacking. The login credentials of many IoT devices, particularly those that are not built with security in mind, are often weak.67 Gateways connecting IoT devices to the manufacturing companies are often insecure.68 Of course, there are vulnerabilities in the devices themselves. Generally, as one commentator has noted, the devices have "a one-time authentication process, which can make them perfect sources of infiltration into company networks."69 Further, the transmission of information often occurs without encryption, creating opportunities for security breaches.70 Part of the problem has been the rapid development of the IoT without a concurrent development in security. Instead, for some of the development of the IoT, security was treated more as an externality, not as an essential component of the core part of the IoT system.71

ii. "Always On" Devices

The expanding "always on" phenomenon of IoT devices is creating significant issues for privacy. It shows that vulnerabilities created by self-surveillance are multiplied by "always on" devices and provide extra targets and opportunities for hacking. Google’s Chromium browser, for example, has code that ensnares private communications72 when a computer’s microphone is turned on without permission.73 Even Mattel’s toy doll, "Hello Barbie," has a Wi-Fi connection and built-in microphone capable of listening to children’s

68 Dickson, supra note 16.
69 Id.
70 Id.
71 Id.
conversations within range to determine a child’s “likes and dislikes.” It is not just toy dolls that listen. Microsoft’s “always on” voice and motion recorder, Kinect, has been installed as part of the company’s Xbox video game console. Of course, Amazon sells its voice activated computer program, Alexa, as a personal assistant who listens for the activating word, “Alexa.” Perhaps the most well-known “always on” device was the Samsung television advertised as listening in on conversations in the same room as the television—and distributing some of those conversations to third parties. To compound the disruptive force of this television feature to privacy, Samsung admitted some of its transmissions were not encrypted.

As “always on” devices proliferate, it will continue to be unclear as to what Americans expect devices to record in their homes, and whether standards will continue to change. The increasing acceptance of these devices, if not the scope of their snooping, creates new understandings of the sanctity and inviolability of the American home.

V. SAFEGUARDING PRIVACY IN AN IOT WORLD

Safeguarding privacy in an IoT world will become increasingly difficult, particularly within the prevailing digital culture of advertising. Right now, tracking incentivizes the continued commoditization of personal information. While some form of disclosure may appear to be in alignment with living “on the grid” in everyday life, privacy issues arise in every stage of information acquisition by a third party—access, storage, analysis, and use. For example, data generated by IoT devices, such as cars, health trackers, and home appliances, could be accessed, saved, and analyzed by life or health insurance companies as well as governments to make critical forward-looking employment, contract, and investigative decisions. Hackers will likely desire access to the same data for monetary or social purposes. With the constraints of living “on the grid” putting all information at risk of disclosure, even the deepest of secrets could be obtained, including those occurring within the furthest reaches of the home.

74 Id. (quoting Iain Thomson, Hello Barbie: Hang On, This Wi-Fi Doll Records Your Child’s Voice? What Could Possibly Go Wrong?, REGISTER (Feb. 19, 2015), www.theregister.co.uk/2015/02/19/hello_barbie/).
75 Id. at 3.
76 Id. at 3–4.
77 Id. at 3.
78 Id. at 5. “It is unreasonable to expect consumers to monitor their every word in front of their home electronics. It is also genuinely creepy.” Id. (citing 2001: A SPACE ODYSSEY (MGM 1968))
79 Meola, supra note 41.
80 Id. For example, German researchers intercepted unencrypted data from a smart meter and determined that the occupant was watching television and learned what show was being watched. Id.
Disseminated by The Research Repository @ WVU, 2017

Friedland: Drinking from the Fire Hose: How Massive Self-Surveillance from t

2017] DRINKING FROM THE FIRE HOSE 907

Protections for such a porous enterprise as the IoT must be structural and not ad hoc. Structural protections can direct privacy shapeshifting through at least four different sources: individuals, companies, the Constitution, and government legislation. Individuals—and the culture they create—can be more vigilant about disclosing information and use new developments in technology to minimize unthinking consent and limit third-party disclosures. Companies can be held accountable for their collection and transfer of information, especially partnerships with government, through interest convergence where privacy is recognized as a legitimate commodity, or the level of company transparency, at least revealing data deletion, use of encryption, whether devices are always on, and if so, what information is within the reach of the devices handled.

Further, government regulations can be enacted to provide informational transparency, both in the collection, storage, and analysis by private companies, as well as the government. While the government has interests in secrecy when information is used for crime interdiction, it can still disclose processes and general outlines of use, such as the scope of government collection, types of use, and longevity of data government receives. Lastly, the Fourth Amendment can be interpreted to rein in the Third Party Doctrine in the new information commodity era, where the coin of the realm is often split-second information available from halfway around the world. Some of these sources will be more viable than others in the near future; others will require long-term percolation. The following subsections will review three of the more likely possibilities: the Fourth Amendment, a culture of vigilance, and company-consumer alliances.

A. The Fourth Amendment as a Protective Source

In the United States, a focal point for privacy over the past several decades has been the Fourth Amendment. While the interpretation of reasonable expectations of privacy has not adapted to the newest technologies, seeds of change have been planted if the courts decide to revisit established search and seizure doctrine. Constitutional interpretation can be applied to the IoT to ensure that reasonable expectations of privacy are maintained despite new waves of technology. Until the Fourth Amendment—or other laws—affords some protection to self-generated data, however, even if that data is voluntarily disclosed in a limited fashion, traditional privacy limits as they currently exist will continue to be ineffective against government intervention. Europe, Australia, and some other countries are beginning to place limits on the scope and nature of use of personal information, crafting legislative norms for informational privacy. Such norms have not been similarly enunciated in the United States. Thus, the most likely short-term protection of privacy in the

United States will have to result from judicial action, the marketplace, or individuals creating a culture of information privacy. Perhaps the most significant leverage point for protection from untrammeled privacy shapeshifting revolves around the Third Party Doctrine of the Fourth Amendment. This doctrine does not provide Fourth Amendment protection to information voluntarily disclosed to a third party. The doctrine has effectively swallowed up much of the discussion about the nuances and intricacies of consent in a digital world.

The doctrine still relies on decades-old cases, such as United States v. Miller, a 1976 case which found that bank records of individuals received no protection against access by the government under the Fourth Amendment, and Smith v. Maryland, a 1979 case that held that pen registers were not within the privacy protected under the Fourth Amendment. The twin pillars of Smith and Miller have been used to justify many forms of bulk data collection. The cases have justified the collection of many terabytes of IoT data and appear to legitimize collection by third parties of much of the data that flows through the IoT as well. The facts of Smith, however, are far removed from justifying bulk self-surveillance data collection without any prior reasonable suspicion of criminal behavior justifying the data collection. The net cast by the IoT cannot be compared to a pen register or paper financial records. The nature and quantity of information created through the IoT allows for a fundamental shift in the nature of police activity.

To illustrate, a man in Ohio was recently charged with aggravated arson and insurance fraud for allegedly burning down his house. A key piece of

---


83 See id.


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


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


89 Bulk data collection can be seen as wholesale, not retail, in that there is no specific criminality that is motivating the police intrusion.

evidence leading to the charge was the information obtained from his pacemaker, which appeared inconsistent with his claim that he was in the house when it caught fire, broke the glass of his bedroom window after packing some belongings, and fled.\textsuperscript{91} The examination of the accused's cardiac rhythms and heart rate at the time of the event, according to a cardiologist, made it "highly improbable" that someone with the accused's heart condition could do what he claimed.\textsuperscript{92} In this case, the police did get a warrant. But if this information were on a device supplied to third parties, such a warrant might be superfluous.

Yet, the foundation for a different approach to information disclosed to third parties was established long ago. Justice Thurgood Marshall, dissenting in \textit{Smith},\textsuperscript{93} stated, "Privacy is not a discrete commodity, possessed absolutely or not at all."\textsuperscript{94} And as one commentator observed,

\[ \text{[T]he idea that information exposed to others is no longer private has been oversold. Millions of Americans expect all sorts of things exposed to third parties remain private under state law. And as technology advances and the information we give to ISPs and telcos becomes more and more revealing, even federal courts are beginning to rethink whether Smith is the absolute rule the government claims it should be.} \]

On its 35th birthday, \textit{Smith}'s vitality is on the decline, and that's a good thing.\textsuperscript{95}

That doctrine, based on cases decided decades ago, such as \textit{United States v. Miller},\textsuperscript{96} does not afford privacy protection to information voluntarily disclosed to third parties.\textsuperscript{97} Through these antecedents, the Third Party Doctrine must be placed within context of the digital era.\textsuperscript{98} While some commentators have advocated abolishing the Third Party Doctrine, others suggest reforming it. One way is to allow for limited disclosures, much like privileged information disclosed to an attorney by a client, a psychotherapist by a patient, or a spouse by another spouse. The level of disclosures sweeps away the private sphere of

\textsuperscript{91} Id.

\textsuperscript{92} Id.

\textsuperscript{93} Smith v. Maryland, 442 U.S. 735 (1979).

\textsuperscript{94} Id. at 749 (Marshall, J., dissenting).


\textsuperscript{96} 425 U.S. 435 (1976).

\textsuperscript{97} See id.

\textsuperscript{98} A promising start to adapting Fourth Amendment doctrine to the digital era was \textit{Kyllo v. United States}, concerning the police's use of a thermal imaging device on a person's home. 533 U.S. 27 (2001). The case was not utilized as a seminal foundation for further applications to the waves of technology.
intimacy which can be protected by a limited disclosure doctrine—particularly if it tracks the protections of well-established privileges.

Another way is to adopt the mosaic test evidenced in the concurrences of Justices Samuel Alito and Sonia Sotomayor in United States v. Jones. The rationale for such a limit was explained by the D.C. Circuit in United States v. Maynard, which observed that long-term surveillance can reveal everything about a person:

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

Justice Sotomayor also advocated that a limited purpose test be adopted in her concurrence in Jones. She wrote:

People disclose the phone numbers that they dial or text to their cellular providers; the URLs that they visit and the e-mail addresses with which they correspond to their Internet service providers; and the books, groceries, and medications they purchase to online retailers... I would not assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection.

Another approach yielding a similar conclusion looks at the value of privacy to democracy and private individuals. If privacy is a highly valued component of

---

100 615 F.3d 544 (D.C. Cir. 2010).
101 Id. at 562 (footnote omitted).
102 Jones, 565 U.S. at 417–18 (Sotomayor, J., concurring).
103 Id.
personal and democratic life, then, just like equal protection analysis, should heightened scrutiny be accorded to some privacy analysis?  

B. A Culture of Vigilance

While laws and the Constitution can shape behavior, perhaps the most pragmatic and immediate privacy protection from a rapidly expanding IoT involves individual action—the creation of a culture of privacy vigilance. The digital culture, seemingly of ubiquitous interconnectedness and sharing without regard to downstream consequences, plays an important role in the massive amounts of data being produced, gathered, and analyzed.

The IoT has exposed the porousness of the current conception of consent, where a single click can lead to the transfer and commodification of huge amounts of personal information over a long period of time. Most people using American websites or apps do not consciously consent to sharing information without limits, or consciously accept the deposit of company trackers, called cookies, or authorize the use of that information downstream. Consequently, traditional legal contours of what counts as acceptable notice likely will not suffice. Instead of marginal minimums, individuals can demand some level of transparency regarding what happens to their information. Much like the common boilerplate offered for the recording of phone calls by companies, “this call is being monitored for quality control and other purposes,” typical website or application consent forms have become more like wallpaper—barely noticed and seldom remembered. Individuals can create some movement in the privacy barometer by at least noticing, and then speaking up.

For many users, the notion of “I have nothing to hide” provides a rationale for permitting disclosure. Yet, the consequences of consent can be significant and adverse, to the extent that individuals do not realize they do have something to protect after all. At least initially, individuals should be reticent to agree to IoT tracking—and that is especially important with respect to sharing that information with third parties. For example, if applications (“apps”) ask permission to have access to contacts, or track individuals even when the app is not being used, the culture should lean away from consenting to the request.


106 Id.
C. Company-Consumer Alliances

Another significant inflection point for privacy and disclosure is the relationship between commercial enterprises that have helped to stoke the gold rush of information and the consumers who create the information. To minimize incentives for companies to participate in the information marketplace and the surveillance economy, privacy needs to be valued by consumers as a commodity in its own right, much like organic foods have become a valued food type. If interest convergence occurs, where company and consumer alignment in interests will occur, even for different reasons, companies will see the value in maintaining the privacy of their customers. This alignment will go a long way to putting some brakes on the flow of information.

There are a variety of ways such an alignment might appear, particularly if consumers are willing to pay for the safeguards. Consumers pay more for organic labels, so perhaps consumers will eventually be willing to pay more for enhanced privacy safeguards. Also, incentives might exist for increasing anonymized information whenever possible. Companies would provide readily understood privacy policies in an accessible place. Companies could disclose with specificity what they actually do with the information, how long that information is held, how it is safeguarded, and who has access to the information. In addition, where and when companies use encryption, how a company deals with government requests for information, whether a company sells the information and if so, to whom, can all be helpful forms of accountability, and elements of a newly constructed privacy norm. While it would be preferable if these requirements were adopted as law, consumers can start showing companies these aspects of privacy matter by indicating as such and showing that privacy is valued with their pocketbooks.

VI. CONCLUSION

The massive production of self-surveillance information as a result of the IoT has changed the face of privacy. The IoT has allowed for data transfers to private companies and, in turn, to the government in unprecedented ways. The IoT has created vast new sources of information through connective radio sensors implanted in every part of a person’s life. That information has become part of the stream of commerce, allowing the government the opportunity to access the information by buying it, grabbing it through an intelligence program, or obtaining it through partnerships with private companies. Sources of self-surveillance often underestimate what happens to their information. The sources can miscalculate the importance of the information collected and IoT devices can raise little fear precisely because the information flow is generally unseen.107

107 Schmidt & Shear, supra note 32.
There is little agreement about what needs to be done, if anything, to safeguard the important personal and democratic value of privacy. Yet, several forms of protection can be adopted to protect against the further dissipation of privacy or its unregulated shapeshifting. Protective tools can emanate from individuals, private companies, the state or federal government, and the Fourth Amendment. While many commentators focus on changing the Fourth Amendment’s Third Party Doctrine to afford more protection to self-generated data, even if that data is voluntarily disclosed in a limited fashion, other sources of protection are available as well. The government can create greater transparency through legislation, but in an age of terrorism and hacking, that is not likely to occur. Instead, the most likely short-term protection of privacy will result from the bottom-up, not the top-down—either from the marketplace with the pragmatic concept of interest convergence, in that the interests of both consumers and companies will become aligned to promote privacy options\(^{108}\) as privacy becomes a more valuable commodity to consumers, or from stronger cultural norms that educate individuals to prioritize the protection of their own privacy.

---

\(^{108}\) Businesses have other incentives to protect privacy of customers. Hackers are a threat to their products, and those companies who encrypt transmissions and allow for password protection from even the companies that make the products—as was illustrated by the Apple iPhone stalemate with the U.S. Government after its attempt to get Apple to overcome a password protecting a terrorist’s phone—will better protect their standing in the marketplace.