INTERNATIONAL JOURNAL OF **OPEN GOVERNMENTS**

REVUE INTERNATIONALE DES **GOUVERNEMENTS OUVERTS**

Vol. 7 - 2018

ISSN 2553-6869

IMODEV
LES ÉDITIONS

International Journal of Open Governments
Revue internationale des gouvernements ouverts

Direction :
Irène Bouhadana & William Gilles

ISSN : 2553-6869

IMODEV
49 rue Brancion 75015 Paris – France
www.imodev.org
ojs.imodev.org

Les propos publiés dans cet article n'engagent que leur auteur.

The statements published in this article are the sole responsibility of the author.

Droits d'utilisation et de réutilisation

Licence Creative Commons – Creative Commons License -

CC-**BY-NC-ND**

Attribution
Pas d'utilisation commerciale – Non Commercial
Pas de modification – No Derivatives

À PROPOS DE NOUS

La **Revue Internationale des Gouvernements ouverts (RIGO)/ the International Journal of Open Governments** est une revue universitaire créée et dirigée par Irène Bouhadana et William Gilles au sein de l'IMODEV, l'Institut du Monde et du Développement pour la Bonne Gouvernance publique.

Irène Bouhadana, docteur en droit, est maître de conférences en droit du numérique et droit des gouvernements ouverts à l'Université Paris 1 Panthéon-Sorbonne où elle dirige le master Droit des données, des administrations numériques et des gouvernements ouverts au sein de l'École de droit de la Sorbonne. Elle est membre de l'Institut de recherche juridique de la Sorbonne (IRJS). Elle est aussi fondatrice et Secrétaire générale de l'IMODEV.

William Gilles, docteur en droit, est maître de conférences (HDR) en droit du numérique et en droit des gouvernements ouverts, habilité à diriger les recherches, à l'Université Paris 1 Panthéon-Sorbonne où il dirige le master Droit des données, des administrations numériques et des gouvernements ouverts. Il est membre de l'Institut de recherche juridique de la Sorbonne (IRJS). Il est aussi fondateur et Président de l'IMODEV. Enfin, il est avocat au barreau de Paris.

IMODEV est une organisation scientifique internationale, indépendante et à but non lucratif créée en 2009 qui agit pour la promotion de la bonne gouvernance publique dans le cadre de la société de l'information et du numérique. Ce réseau rassemble des experts et des chercheurs du monde entier qui par leurs travaux et leurs actions contribuent à une meilleure connaissance et appréhension de la société numérique au niveau local, national ou international en en analysant d'une part, les actions des pouvoirs publics dans le cadre de la régulation de la société des données et de l'économie numérique et d'autre part, les modalités de mise en œuvre des politiques publiques numériques au sein des administrations publiques et des gouvernements ouverts.

IMODEV organise régulièrement des colloques sur ces thématiques, et notamment chaque année en novembre les *Journées universitaires sur les enjeux des gouvernements ouverts et du numérique / Academic days on open government and digital issues*, dont les sessions sont publiées en ligne [ISSN : 2553-6931].

IMODEV publie deux revues disponibles en open source (ojs.imodev.org) afin de promouvoir une science ouverte sous licence Creative commons CC-**BY-NC-ND** :

1) la *Revue Internationale des Gouvernements ouverts (RIGO)/ International Journal of Open Governments* [ISSN 2553-6869] ;

2) la *Revue internationale de droit des données et du numérique (RIDDN)/International Journal of Digital and Data Law* [ISSN 2553-6893].

ABOUT US

The **International Journal of Open Governments / Revue Internationale des Gouvernements ouverts (RIGO)** is an academic journal created and edited by Irène Bouhadana and William Gilles at IMODEV, the Institut du monde et du développement pour la bonne gouvernance publique.

Irène Bouhadana, PhD in Law, is an Associate professor in digital law and open government law at the University of Paris 1 Panthéon-Sorbonne, where she is the director of the master's degree in data law, digital administrations, and open governments at the Sorbonne Law School. She is a member of the Institut de recherche juridique de la Sorbonne (IRJS). She is also the founder and Secretary General of IMODEV.

William Gilles, PhD in Law, is an Associate professor (HDR) in digital law and open government law at the University of Paris 1 Panthéon-Sorbonne, where he is the director of the master's degree in data law, digital administration and open government. He is a member of the Institut de recherche juridique de la Sorbonne (IRJS). He is also founder and President of IMODEV. He is an attorney at law at the Paris Bar.

IMODEV is an international, independent, non-profit scientific organization created in 2009 that promotes good public governance in the context of the information and digital society. This network brings together experts and researchers from around the world who, through their work and actions, contribute to a better knowledge and understanding of the digital society at the local, national or international level by analyzing, on the one hand, the actions of public authorities in the context of the regulation of the data society and the digital economy and, on the other hand, the ways in which digital public policies are implemented within public administrations and open governments.

IMODEV regularly organizes conferences and symposiums on these topics, and in particular every year in November the Academic days on open government and digital issues, whose sessions are published online [ISSN: 2553-6931].

IMODEV publishes two academic journals available in open source at ojs.imodev.org to promote open science under the Creative commons license CC-**BY-NC-ND**:

1) the *International Journal of Open Governments*/ la *Revue Internationale des Gouvernements ouverts (RIGO)* [ISSN 2553-6869] ;

2) the *International Journal of Digital and Data Law* / la *Revue internationale de droit des données et du numérique* (RIDDN) [ISSN 2553-6893].

TRANSMOGRIFYING PRIVACY: THE IMPACT OF THE INTERNET OF THINGS ON OPEN GOVERNMENT

by **Steven I. FRIEDLAND**, Professor in Law at Elon University, USA.

Privacy can be seen as both a personal right and an important pillar of open government. Yet, understandings of privacy are changing at breakneck speed in the digital era. In essence, privacy has become transmogrified; a shapeshifter. A particularly transformative influence has been the Internet of Things (IoT). The IoT, a series of networks often but not always connected through the Internet, have opened a firehose of information for companies and governments alike. This treasure trove of information allows for government tracking in unprecedented ways. This paper 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.

We live in a volatile world of diminishing privacy. Part of the reason lies with the enormous data flows created by the Internet and connecting devices, often labeled the Internet of Things (IoT). These data flows become part of information marketplaces, and often find their way to the government. Thus, the IoT, for all its progressive digital advantages, has become a huge feeder of information to private companies and the government, generally without any of the traditional safeguards of privacy, such as the Fourth Amendment's requirement of probable cause or warrants for many searches. Controlling this IoT-enhanced information flow to government will be critical in coming years to maintaining open government, which otherwise could access information equivalent to serving general warrants, as was common in pre-United States England.

The IoT, meaning the world of networks connected to each other through the Internet or other radio transmission devices, creates consensual mass self-surveillance systems in numerous and growing domains. Just observe the fitness industry and the ubiquitous Fitbit, creating a wealth of portable health information, the auto industry and "smart" cars, creating consumable information about driving habits, cell phones and real-time location information, and the fashion industry and smart wearables, from watches to shirts, producing waves of information about personal habits. There are even "smart" houses and cities, revealing clues to city functioning.

The exponential increase in interconnectivity resulting from advancing technologies, combined with the rise of mass self-cybersurveillance, have served to dramatically change the calculus in the protection of personal privacy, exposing more data to

others than ever before. The treasure trove of information created by the IoT, in particular, allows for government tracking in unprecedented ways.

The paper explores the influence of the IoT on privacy and open government, particularly the mass self-surveillance it produces and the new shapes of privacy that are emerging as a result. To protect privacy and maintain government transparency, this paper advocates the minimization of vulnerabilities of the IoT, the fortification of consent, and the creation of structural controls by law.

§ 1 – BACKGROUND

A) The Information Society

1) Data Everywhere

While physical walls and doors once protected our personal secrets from governments, commercial enterprises and nosy neighbors alike, today, our cyber-connected world has created data flows that are as large as oceans and as fast as jet planes. If a person lives on the "grid", their intimate, personal and valued information is subject to disclosure to third parties—and the eventual sale or distribution to others far downstream of its intended disclosure. The Internet has created a global conduit for information creation, aggregation, storage and analysis with methods that are more efficient and swifter than ever before. The potential for disruption of privacy is considerable[1].

2) Built-in Surveillance with the Internet: the Big Flaw

A significant predicate of much of the cybersurveillance occurring today was the decision to allow users of the Internet to access it for "free", meaning no payment was required for use. This use-for-free concept does not indicate the true costs of access, however, because what the real payment is involves the opportunity to track users — their preferences, habits, and propensities. This conceptualization created a system of tracking that proliferated and became firmly entrenched in the online culture. The user information is tracked even when the users leave and go to other sites through "cookies", or small files that identify and tag users.

[1] J. MANYIKA et al., *Disruptive Technologies: Advances that Will Transform Life, Business, and the Global Economy* 2-3 (2013), *available at* http://www.mckinsey.com/~/media/mckinsey/dotcom/insights%20and% 20pubs/mgi/research/technology%20and%20innovation/disruptive% 20technologies/mgi_disruptive_technologies_full_report_may2013.ashx, <http:// perma.cc/N9AP-28RW>. These technologies are transformative because they contribute to social change, where new ways of doing things supplant the status quo, "rendering old skills...irrelevant". *Ibidem.* at 1. In fact, mobile Internet and Cloud technologies are advancing at an explosive rate and, together, have created a culture of users who "go about their daily routines with new ways of knowing, perceiving, and even interacting with the physical world". *Ibidem.* at 6.

3) Data Marketplaces

a. Private Multinational Companies

Private multinational companies often receive the most notoriety about the data they collect, transfer and sort. Even free applications are not really "free" — the Internet has built-in costs. User information is so valuable it is often bartered, sold, and transferred, joining the stream of data in the information marketplace, where it is parsed by algorithms, sorted and recombined to yield additional information. The marketplace transfers that information to others, often at a profit. The IoT has been a peculiar source of regular information — showing that data marketplaces are now sourced by self-surveillance information as much as that created by third-party hackers or eavesdroppers.

b) The Government

Various agencies in the U.S. government engage in procuring information through public-private partnerships with companies or with other governments[2]. This information supplements direct surveillance on individuals, from face recognition systems, to breaking into vulnerabilities of other systems, to officially obtained subpoenas and warrants to search for particular information.

In 2015, the Internet media company, Yahoo, Inc., secretly created a software program that searched its customers' incoming emails in real-time on behalf of U.S. government email surveillance. The classified government directive that resulted in the spying emanated either from the NSA or the FBI[3]. Instead of Yahoo fighting the government request for investigative cooperation, the encryption of the incoming emails received by Yahoo customers was circumvented — by Yahoo itself. Yahoo scanned hundreds of millions customer emails without their knowledge. Unlike what is known about requests for previously sent emails, this one involved all incoming emails in real time, an apparent first of its kind, not simply a circumscribed subset of incoming emails or stored emails.

The source of federal power for the secret conscription of Yahoo, Inc. was apparently the Foreign Intelligence Surveillance Act through the Foreign Intelligence Surveillance Court. Because of

---

[2] *See* B. FUNG, *What to Expect Now that Internet Providers can Collect and Sell Your Web Browser History*, Wash. Post (March 29, 2017) https://www.washingtonpost.com/news/the-switch/wp/2017/03/29/what-to-expect-now-that-internet-providers-can-collect-and-sell-your-web-browser-history/?utm_term=.98d9f4bb39f8. See also, C. SAVAGE, N. PERLROTH, *Yahoo Said to Have Aided U.S. Email Surveillance by Adapting Spam Filter*, N.Y. Times (October. 5, 2016) https://www.nytimes.com/2016/10/06/technology/ yahoo-email-tech-companies-government-investigations.html..

[3] J. MENN, *Exclusive: Yahoo Secretly Scanned Customer Emails for U.S. Intelligence – Sources*, Reuters (October. 4, 2016, 1:04 PM) http://www.reuters.com/article/us-yahoo-nsa-exclusive-idUSKCN1241YT.

the secrecy, it is unknown whether the government had made this request of other telecoms and Internet companies as well.

The software program searched for certain 'digital signatures' in the emails associated with a state-sponsored terrorist organization. If the program found the specific signatures, the system copied and saved the emails[4].

The U.S. Government denied any impropriety. A spokesperson for the U.S. Office of the Director of National Intelligence stated: "The United States only uses signals intelligence for national security purposes, and not for the purpose of indiscriminately reviewing the emails or phone calls of ordinary people"[5].

Yet, it was none other than Edward Snowden, who had leaked a massive amount of classified documents in 2013 that disclosed widespread NSA intelligence programs, who put the spying in a transparency perspective. Speaking to students at Georgetown University via satellite, Snowden said the Yahoo situation raised questions once again about whether government surveillance programs have adequate transparency due to "congressional oversight and public scrutiny"[6].

Congressional intelligence committees in the House of Representatives and the Senate have begun to investigate how Yahoo came to create this customized program.[7] Of course, the subsequent investigation is consonant with Snowden's point — that Congress is often one step behind and has insufficient real-time knowledge of the breadth and depth of intelligence community programs.

To deal with such situations, there must be a greater predicate than a single judicial order without any limitations on the number of emails searched, how long the search occurs and who gets to know about the search. While secrecy is important in the content of the search, keeping the information in a complete shadow, shielded from government or public scrutiny, is anathema to the Fourth Amendment and due process clauses.

In addition to the Yahoo real-time surveillance at the behest of the U.S. intelligence community, a government purchase of surveillance in the commercial marketplace illustrates a very different type of surveillance. In this case, a software program based on surveillance of individuals by a private company to assign people 'threat scores' was purchased by some U.S. police departments to assist with responses to 911 calls[8].

---

[4] C. SAVAGE, N. PERLROTH, *Yahoo Said to Have Aided U.S. Email Surveillance by Adapting Spam Filter*, N.Y. Times (October. 5, 2016) https://www.nytimes.com/2016/10/06/technology/yahoo-email-tech-companies-government-investigations.html.

[5] *Ibidem.*

[6] See M. HOSENBALL, D.VOLZ, *Yahoo Email Scan Fell Under Foreign Spy Law – Sources*, Reuters (October. 5, 2016, 6:13 PM) http://www.reuters.com/article/us-yahoo-nsa-idUSKCN1252NR.

[7] *See* M. HOSENBALL ,D. VOLZ, *Yahoo Email Scan Fell Under Foreign Spy Law – Sources*, Reuters (October. 5, 2016, 6:13 PM) http://www.reuters.com/article/us-yahoo-nsa-idUSKCN1252NR.

[8] J. JOUVENAL, *The New Way Police Are Surveilling You: Calculating Your Threat 'Score'*, Wash. Post (January. 10, 2016) https://www.washingtonpost.com/local/public-

The company, Intrado, created the Beware software program to determine the level of dangerousness of individuals, particularly when confronted by police officers responding to a 911 call. It is proprietary software, and therefore its processes remain undisclosed — from competitors, as well as those it characterizes and classifies.

B) Self-Surveillance Systems and the IoT: A New Source of Information

1) The IoT

Rather than simply consisting of things connected to the Internet, the Internet of Things is actually broader and less contained. The basic component of the Internet of Things consists of a group of devices connected to the Internet through local Internet Protocol (IP) addresses, but it also includes any devices connected by radio transmitters to a network for a specific purpose. While some of these 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 Internet of Things can be found — even if the device is not measuring a thing, but rather an intangible, like the wind or sleep practices.

A common thread throughout the Internet of Things networks is the presence of semi-autonomous data-generating sensors. The sensors in the devices have specific purposes. For example, a smart thermostat does not simply monitor temperature, but learns to do so when the temperature actually matters, such as when the residents of the home or office are present. A car might have special sensors for its backup camera to assist the car in reverse, and a radar system to determine what cars are passing it on either side, to minimize "blind" spots. These features are automated to a large extent, allowing some devices to operate remotely.

The sensors connect through tiny radio transmitters over networks. These networks, like train systems, include the Internet and Local Area Networks (LAN). Often, the transmitter will connect through Wireless Fidelity (Wi-Fi),[9] but can communicate through a less powerful connection, such as Bluetooth transmission.

A key to understanding the devices within the Internet of Things is that they are generally multifunctional,[10] such that their form and function are distinct. A smart watch offers the time, but also

safety/the-new-way-police-are-surveilling-you-calculating-your-threat-score/2016/01/10/e42bccac-8e15-11e5-baf4-bdf37355da0c_story.html?utm_term=.a3c70a4c631f.

[9] E. A. FISCHER, Cong. Research Serv., R44227, The Internet of Things: Frequently Asked Questions 3 (October. 13, 2015), https://fas.org/sgp/crs/misc/R44227.pdf.

[10] For example, many household appliances, watches, cell phones, cars, and clothing are all connected to networks, providing them with multiple functions.

might provide the temperature, text messages and email[11]. A smart car transports its occupants, but also can have systems that collect and transmit data for specific functions, such as automated backup cameras, radar detection, and brake sensors. The smart television sets provide programming, but also can be triggered remotely by commands from voice activation.

Thinking of the Internet of Things as a singular entity also misses the mark. The nature and scope of the connected devices often depend on the particular industry or domain within which the devices operate.[12] The devices are purposed within the context of the setting and are automated to collect and transmit data for a specific reason. That is why there are different types of interconnectivity within a 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), businesses, and even cities (for electric grids and security). That is also why a common 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 the way devices can communicate and connect with each other to collect, sort and transmit data. Perhaps the most that can be said about the Internet of Things is that as it continues to grow, its definition will evolve. The flow of information created by the IoT, though, extends not only to private companies, but to governments as well. Significantly, much of the information flow to government is beyond the glare of public openness.

2) Self-Cybersurveillance and the IoT

A central feature of IoT systems is that they are often create voluntary self-surveillance. That is, the subjects either initiate surveillance (e.g., put on wearable tech or buy smart appliances), or readily consent to surveillance (e.g., html cookies deposited in web sites). The information then starts flowing by being consensually shared with the application maker or software manufacturer, which often finds its way into the information marketplace. The information stream can then continue moving, from within the industry domain and on to the government.

---

[11] *See, e.g.*, *Apple Watch*, Apple, http://www.apple.com/watch/?cid=wwa-us-kwg-watch-co.

[12] This notion applies to cellular telephones. For instance, Near-Field Communication (NFC) allows direct cell phone-to-cell phone communication. J. BRANDON, *8 Groundbreaking Mobile Tech Advancements for 2012*, POPULAR MECHANICS (January. 28, 2013), *available at* www.popularmechanics.com/technology/gadgets/news/8-groundbreaking-mobile-tech-advancements-for-2012#slide-1. Other expanding technologies include a Bluetooth health-device protocol that connects a phone to heart monitors and cardio equipment. Mobile security through CarrierIQ has been developed, as have smart skin phones that take any digital image and display it across the skin of the phone.[12] There is also a combination phone, laptop tablet and digital camera. *See, e.g.*, *Runtastic Heart Rate Combo Monitor,* RUNTASTIC SHOP, https://www.runtastic.com/shop/en/runtastic-blue-bluetooth-smart-combo-heart-rate-monitor?utm source=runtastic.com&utm medium=l ink&utm campaign=shop.runbt1&utm content=static/show.products page.

§ 2 – ISSUES CREATED BY THE IOT

A) Vulnerabilities[13]

The increasing reliance on advancing technologies promotes vulnerabilities in networks,[14]. As long as there are people who like "smart" devices and remote operability, hackers will attempt to take advantage, particularly as ransomware becomes more sophisticated and profitable. Many people still do not protect their devices, which is like leaving the front door wide open to a house, and phishing schemes are very common.

Internet-related networks are increasingly vulnerable to hacking.[15] Hacking, essentially modern thievery, can result in loss of information, stolen identities and, increasingly, ransom plots to retrieve use of 'frozen' computers. Common coding methods make it easier for hackers. As one commentator noted:

Every time you search for something on Google, hail an Uber or log into a bank account, your personal data likely flow behind the scenes through a series of separate, freestanding packages of software known as containers. Although invisible to the user, this method has become the dominant way to code apps today. Programmers like it because it allows them to change one feature without breaking their colleagues' work, and it helps software run more efficiently, saving companies money[16].

The vulnerabilities arise in different ways[17]. According to the Federal Trade Commission:

IoT devices may present a variety of potential security risks that could be exploited to harm consumers by: (1) enabling unauthorized access and misuse of personal information; (2) facilitating attacks on other systems; and (3) creating safety risks.

---

13 D. VOLZ, *U.S. Senators to Introduce Bill to Secure 'Internet of Things'*, Reuters (August. 1, 2017, 8:04 AM) https://www.reuters.com/article/us-usa-cyber-congress-idUSKBN1AH474..

14 J. SCHLESCHINGER, "New Hacking Threats: Fingerprint Reader Vulnerabilities and Sophisticated Ransomware," CNBC Business (May 20, 2017). "It is going to get worse before it gets better because we've becoming more reliant [on technology]… More sophisticated attacks will be hard to prevent", said Stuart Okin, a senior vice president of product at 1E, a cybersecurity firm that helps companies keep software up to date.

15 A. GREENBERG and K. ZETTER, *How the Internet of Things Got Hacked*, Wired (December. 28, 2015 7:00 AM), https://www.wired.com/2015/12/2015-the-year-the-internet-of-things-got-hacked/.

16 J. ROBERTSON, *The Latest Coding App Trend Is a Hacker's Dream*, BLOOMBERG: TECHNOLOGY (July 17, 2017 12:01 AM), https://www.bloomberg.com/news/articles/2017-07-18/the-latest-app-coding-trend-is-a-hacker-s-dream.

17 FTC Staff Report, "Internet of Things: Privacy and Security in a Connected World", at 12 (2015). Found at: https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf . "Participants also noted that privacy risks may flow from the collection of personal information, habits, locations, and physical conditions over time. In particular, some panelists noted that companies might use this data to make credit, insurance, and employment decisions. Others noted that perceived risks to privacy and security, even if not realized, could undermine the consumer confidence necessary for the technologies to meet their full potential, and may result in less widespread adoption." At ii.

Although each of these risks exists with traditional computers and computer networks, they are heightened in the IoT[18] .
This package approach is now used by an estimated quarter of all large companies, and is expected to keep growing[19]. Companies focus on increasing their technology, often at the expense of the ways to make it secure[20].It makes creation easier, but it also makes disruption easier as well. As the same commentator notes:
But the process is also giving hackers lots of new ways to steal people's information. Instead of a user's data going directly to one place, they can jump between dozens of containers for a single action. Hackers only need to gain access to one. Because of the way most containers are designed, they're black boxes on a network[21].

B) Weak Consent

The ready availability of consent with a single click of a mouse, as well as bottlenecks for social media and culture by behemoth companies like Google, Apple, Amazon, and Instagram, have contributed to the weak consent to waive protection of personal information. It is no wonder that consent to disclose information to others—and permanently lose privacy protection over it—is weaker than other forms of waiver protection.
Thousands of searches occur by the government without a warrant due to consent[22]. As one commentator noted, "The question of voluntariness is difficult to assess, however, despite attempts by appellate courts to provide guidepost factors for trial court analysis"[23]. The seminal case, Schneckloth v. Bustamonte,[24] involved six men stopped at 2:40 a.m. by the police in a car. An officer asked one of the passengers if the officer could search the car without informing the person that he could say no. The Supreme Court held that based on a totality of the circumstances, all that was needed was voluntariness; informing the person of their right to refuse was not required[25]. Factors in determining voluntariness include:
the use of violence or threats of violence; the police's use of and the defendant's reliance upon promises, deception, or claims that a warrant is obtainable; whether the defendant was in custody at the time of consent; the defendant's physical or mental condition; the location where consent was given; the defendant's level of

[18] FTC Staff Report, "Internet of Things: Privacy and Security in a Connected World," at 12 (2015). Found at: https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.
[19] *Ibidem.*
[20] *Op.cit.*
[21] *Op.cit.*
[22] B. A. SUTHERLAND, "Whether Consent to Search Was Given Voluntarily: A Statistical Analysis of Factors that Predicts the Suppression Rulings of Federal District Courts", N.Y.U. L. Rev. 2192 (2006).
[23] *Ibidem.* at 2192.
[24] *Schneckloth v. Bustamonte*, 412 U.S. 218 (1973).
[25] *Ibidem.* at 2196.

cooperation; the defendant's understanding or awareness of the right to refuse to consent; and the defendant's belief that no incriminating evidence would be found[26].

The consent required to waive rights at trial, on the other hand, is more fortified, and must be knowing, intelligent and voluntary[27]. The waiver of the Fifth Amendment privilege against self-incrimination under Miranda v. Arizona[28] requires giving several warnings to persons subject to custodial interrogation, in whatever the language the person interrogated understands.

The consent required for information produced by the IoT, in particular, does not require any formality at all. Nor is there a requirement that the person have understanding of what is waived, or that receipt of the information by the government requires a higher standard[29].

Thus, it is profoundly easy for people to "agree" to privacy rules in a long and detailed consent form—with the alternative being unable to obtain access to a website that is part of a peer culture, financial base, or other site important for functioning in everyday life. The difficulty of sorting through the terms—words and phrases that may be filled with legalese and complex concepts—when balanced against the ease of a single click acceptance, contributes to the unevenness of the playing field. Further, the decision to agree or not agree to regulations is without context—it is done in isolation, without others providing comment or influence. This type of isolation was derided by Chief Justice Warren in Miranda v. Arizona[30], suggesting that the isolation of police custodial interrogation warranted the giving of warnings—prophylactic safeguards—before finding that statements by subjects are voluntary[31].

C) Impacting Open Government

Governments are collaborating with companies, other countries, and others to obtain IoT user information, as well as accessing information directly. While some of the accessing of information would be justified under the stringent standards of the Constitution and statutes, much of it is gratuitous and not particularized, related to specific criminal investigations. This accumulation of data without a specific purpose equates to the general warrant of old, executed often as an oppressive tool in Britain before the colonies broke away to form the United States.

Further, with website access, it is convenient to quickly check a consent box without reading the lengthy terms and conditions associated with the use of the site. Even when it is read, the user has great incentive to agree or else be denied access from

[26] *Ibidem.* at 2197, Note 31.
[27] See, e.g., *Johnson v. Zerbst*, 304 U.S. 458 (1938).
[28] *Miranda v.* Arizona, 384 U.S. 436 (1966).
[29] See, e.g., *Schneckloth v. Bustamonte*, 412 U.S. 218 (1973).
[30] *Ibidem.*
[31] *Ibidem* at 462.

important portals in the mainstream culture, from social media, to on-line banking, shopping, education and all other aspects of participating in society.

The information generated by IoT transmitting devices easily can be shared with application developers, manufacturers, and other third parties. The data trail often is invisible. Unlike a police tail or cameras fixed on buildings, the surveillance from the interconnected devices lies submerged and unseen, like an odorless gas. The devices can raise little fear precisely because the potential harms from shared information are unseen and often surface far downstream.

Yet, open government is an important feature in a democratic system. It allows constituents to determine if representatives are indeed representing the interests of the populace and are worthy of reelection. Representing the interests of constituents means not just of the individuals, but of the state as a whole. Further, to minimize abuses, a broad system of checks and balances, Separation of Powers, was instituted. Without some degree of transparency, it would be difficult if not insuperable to determine if the government is eliding abuses and engaging in their proper and limited roles.

1) Porous Privacy Safeguards[32]

Government-imposed consumer safeguards are not equipped to deal with the vulnerabilities of the IoT, the sophisticated means by which hackers can access the personal data of others, and the weak obstacle of one-click consent to disclosure and sharing of information with other that is the gateway to using sites on the Internet.

The Fourth Amendment has created privacy that protects people, not necessarily the IoT. The seminal cases remain moored in the 20th Century[33]. Thus, when there is consent to disclosue information, it can readily and lawfully find its way to the government, sight unseen.

2) How the IoT Undercuts Open Government

The interconnecting devices of the IoT create multiple levels of self-mass surveillance. Some mass surveillance systems are micro-oriented, such as how active a person is who wears a cyberonic device like a FitBit, and some are macro-oriented, such as monitoring an area of a city for electricity consumption, traffic patterns, and criminal activity[34]. The micro-oriented surveillance

[32] S. WEISMAN, *Are you Safe in the Internet of Things*, USA Today (April 4, 2015, 9:02 AM) https://www.usatoday.com/story/money/columnist/2015/04/04/weisman-internet-of-things-cyber-security/70742000/.

[33] See e.g., Katz v. United States, 389 U.S. 347(1967).

[34] *See, e.g.*, *Surveillance Society: Wearable Fitness Devices Often Carry Security Risks*, Pittsburgh Post Gazette (August. 3, 2015), http://www.post-gazette.com/news/surveillance-society/2015/08/03/Surveillance-Society-Wearable-fitness-devices-often-carry-security-risks/stories/201508030023.

often becomes a layer of larger systems. To illustrate, the heart-tracker joins with blood pressure evaluation, sleep assessor and step measurer to create a better gage of personal health.

A central feature of these structures is that they are often constructed using voluntary self-surveillance facilitated by the Internet of Things. 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 web sites). The information then is consensually shared with the application maker or software manufacturer, and often wends its way into the information marketplace — and to the government. The information stream can then move from within the industry domain to the government. While this flow of information is often understated or hidden to the common user, even when that is not the case, the significance of the downstream flow of information is not fully grasped by many users — especially those enthralled with the IoT and its promises[35].

§ 3 – Possible Responses to Protect Data Privacy and Open Government From IoT Vulnerabilities

A) A Pragmatic Response: Minimize Vulnerabilities of the IoT

Much like roads and bridges that deteriorate after extensive use, there ought to be some governmental and private response to the vulnerabilities that are being built into the infrastructure of the IoT. While inexpensive radio transmitters and other parts decrease costs of the IoT, in the long run, they are more costly given the expense for leaking data. As expects know, zero days, and other kinds of vulnerabilities are being preyed on by hackers and governments on a regular basis. These vulnerabilities are proliferating because sellers are prioritizing cost of devices over security[36].

In particular, there must be regular updating of software and regular patching of vulnerabilities, once found or known. As one commentator noted:

But what if devices were even more vulnerable, running with no built-in security and no opportunity to patch? This is the problem that that the so-called internet of things (IOT) presents. With an anticipated 22.5 billion devices due to be connected to the

[35] One example is the web site, thenextweb.com (TNW). 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 also do share that information with third parties for ads and analytics". See, TNW,. http://thenextweb.com/insider/ (last visited September. 15, 2016).

[36] *Ibidem*. "One approach to driving up standards in cyber security is through the insurance industry. Firms such as QBE and AIG have been examining the role that they can have in protecting consumers and companies against cyber threats, contributing to the development of a required culture of cyber security that ceases to prioritize the affordability of products over security".

internet by 2021, the opportunity for holding these devices to ransom will present significant opportunities to criminals and will have serious consequences for providers and users of these devices[37].

Legislation can ensure updating and patching, and should be implemented for all companies on a reasonable basis. So can modified regulations involving the insurance industry, which can help consumers and change the cyber security culture to ensure that sensors are properly secured[38]. This culture, though, is driven by the proliferation of computers that can be attached now to all kinds of things. As one commentator observes:

"We no longer have things with computers embedded in them. We have computers with things attached to them." This includes increasingly household fixtures, implanted and wearable medical devices, smart cities where public services utilize technology with the aim of improving efficiency and quality, and critical national infrastructure, such as power grids and railway systems » [39].

Promote Informed Consent and Fair Information Practice Principles[40].

Consent is a legal term that allows for the waiver of rights and interests. What constitutes consent is an issue in many legal areas and in other domains, such as bio and medical ethics, where informed consent by patients, subjects and others is treated with great care[41]. While consent can be seen in property law in gifts and entry onto property, and in contract law with basic formation, it is a prevalent means by which a great deal of information joins the information marketplace. With the help of legislation, consent can be translated into a cornerstone of an online privacy bill of rights.

There are varying safeguards in the law for informed consent. There are greater protections, for example, when a person is the subject of police interrogation or waiving trial rights. There is lesser protection when it involves disclosures of information to third parties, on the Internet or off it.

The constitutional rights safeguarded under Miranda v. Arizona[42], for example, provide a parallel for fortifying informed consent. If consent can lead to prosecutions, such as requests to search a car

---

37 H. BRYCE, " The Internet of Things Will Be Even More Vulnerable to Attack", Chatham House (May 18, 2017). Found at: https://www.chathamhouse.org/expert/comment/internet-things-will-be-even-more-vulnerable-cyber-attacks.

38 *Ibidem.*

39 *Ibidem.* Quoting security expert BRUCE SCHNEIER.

40 FTC Staff Report, "Internet of Things: Privacy and Security in a Connected World," at ii (2015). Found at: https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf "In addition, workshop participants debated how the long-standing Fair Information Practice Principles ("FIPPs"), which include such principles as notice, choice, access, accuracy, data minimization, security, and accountability, should apply to the IoT space. The main discussions at the workshop focused on four FIPPs in particular: security, data minimization, notice, and choice. Participants also discussed how use-based approaches could help protect consumer privacy".

41 See, e.g., NC MANSON and O. O'NEIL, *Rethinking Informed Consent in Bioethics* (Cambridge U. Press 2007).

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

or home, then the results can be just as invasive as that which occurs during custodial interrogation.

While the Supreme Court found that consent to search need not involve a higher order of safeguards in Sneckloth v Bustamonte,[43] several aspects of that case suggest it should no longer be followed. First, the case was decided in 1973, well prior to digitization, cellular telephones, and the Internet. The sea change that has occurred with the flood of technology warrants reconsideration of consent requirements. Second, the case involved the search of a car that had been stopped for traffic violations, a very narrow vehicle for understanding consent in a plethora of other situations[44]. Even when viewed through the lens of traffic stops, today's sometimes inflammatory confrontations between police and citizens in traffic stops warrants reworking even the core analysis in that case. Further, the racial, power disparity, and sociopolitical narratives cannot be ignored in analyzing "voluntariness" based on a "totality of the circumstances. These nuances multiply when considering Big Data and the algorithms used to sort the data and draw inferences and predictions from it[45].

1) Promote Notice as Part of Informed Consent

Informed consent to disclose data, then, can be strengthened by adding a notice requirement. Consumers must be first be notified "when sensitive data is collected or where there is unexpected collection or sharing" – especially by the government[46]. The Federal Trade Commission values notice in its framework, and that requirement should be extended to potential disclosures of sensitive personal information[47]. While some argue that a multiplicity of notice requirements would be counterproductive,[48] ensuring rights to choose not to disclose would better articulates the ownership conception of data.

Further, if the government had to provide notice of the types of data it has collected, screened for national security issues, this would hold the government more accountable and minimize government fishing expeditions for data. This notion is predicated on the view that if the government has no checks in acquiring data, then there will be no balance that results.

---

[43] *Sneckloth v Bustamonte*, 412 U.S. 218 (1973).

[44] *Ibidem.*

[45] *See, e.g.,* K. GOLEMBIEWSKI, "All data are not created equal: upholding the Fourth Amendment's guarantees when third party consent meets the shared electronic device" 56 WASHBURN L.J. 35-67 (2017).

[46] G. CORAGGIO & K. LUCENTE, *The Internet of Things: EU vs US Guidance*, 20 No. 6 Cyberspace Lawyer NL 7 (2015).

[47] *Ibidem.*

[48] See generally, J. BRONFMAN, *Weathering the Nest: Privacy Implications of Home Monitoring For the Aging American Population*, 14 Duke L. & Tech. Rev. 192, 217 (2016).

2) Other Factors

Informed consent also can benefit from a time delay – e.g., even a waiting period of several minutes -- or required consideration of factors prior to a waiver, such as accessibility, purpose of disclosure, and willingness to share to other third parties. For example, the notice requirement can be interposed when one device attempts to share information with another device[49]. These cross-context uses can be brought into the sunlight with a consent requirement, minimizing what falls into government data banks, particularly if it is framed within legislation[50].

Legislation can promote this kind of informed consent, either by requiring a delay in time or consideration of some factors, legislation will help limit companies and governments, and make data transmission more transparent. This transparency will illuminate violators, but also provide settled expectations that do not exist at the present.

CONCLUSION

The IoT comprises a huge wave of technology in the future of a connected world. Yet, for all of its advantages and perceived benefits, it has potentially great costs as well, especially related to self-surveillance and open government. Without attention and oversight, and safeguards such as stronger consent and minimization of network vulnerabilities to hacking, open government will be much more difficult to achieve. Before data surreptitiously enters the stream of commerce, greater consent hurdles must be erected to maintain the balance between disclosure and privacy.

[49] S. R. PEPPET, *Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent*, 93 Tex. L. Rev. 85, 140 – 144, at 150-157 (2014).
[50] *Ibidem.*