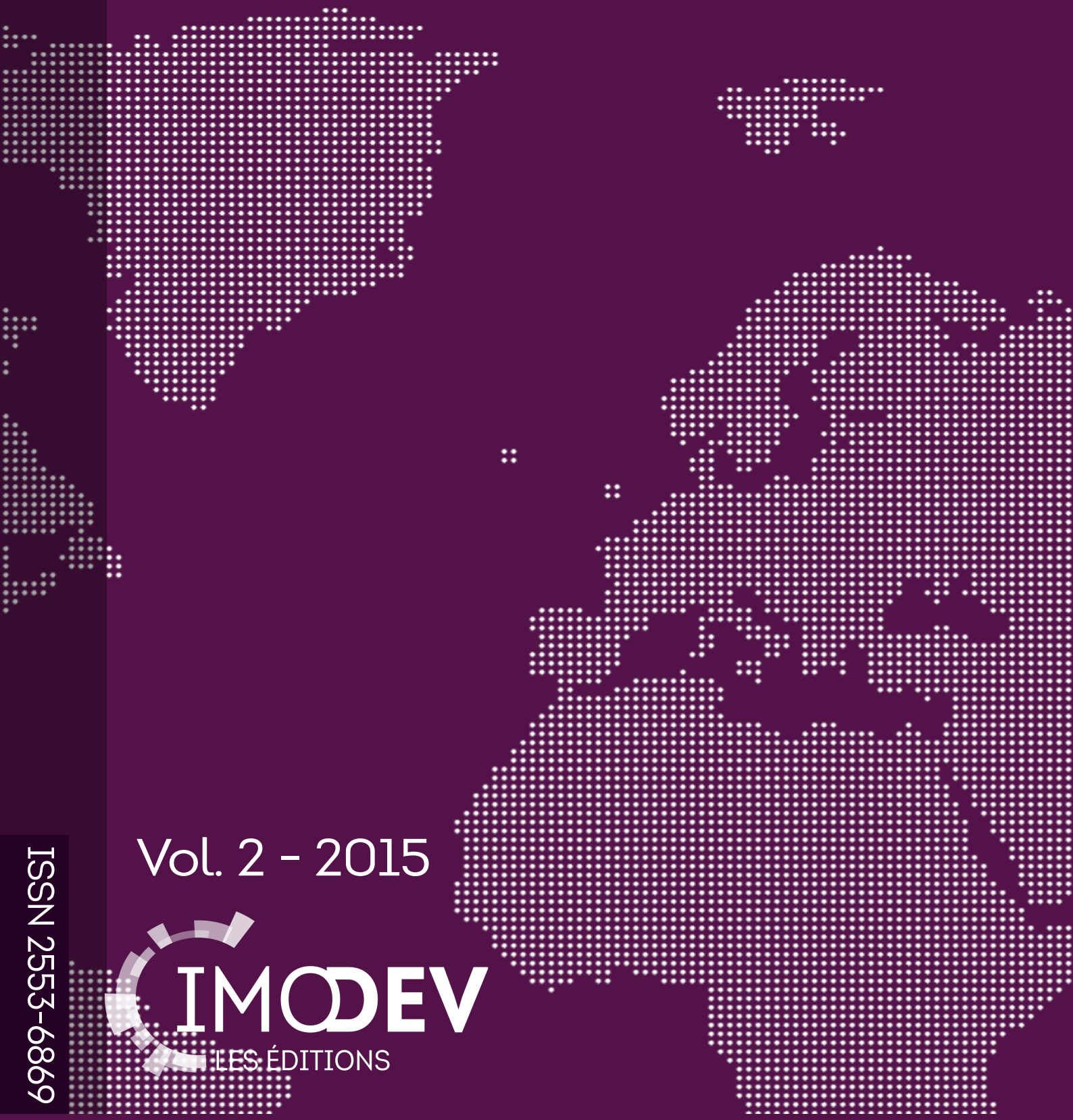
INTERNATIONAL JOURNAL OF **OPEN GOVERNMENTS**

REVUE INTERNATIONALE DES **GOUVERNEMENTS OUVERTS**



Vol. 2 - 2015

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.

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.

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.

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] ;

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

UNCHECKED AND UNBALANCED: THE ADVERSE IMPACT OF CYBERSURVEILLANCE ON GOVERNMENT TRANSPARENCY

by **Steven I FRIEDLAND**, Professor of law and senior scholar at the Elon University

INTRODUCTION

General Michael Hayden (ret.), the former director of the National Security Agency, recently told a gathering that what is "reasonable" for searches and seizures under the Fourth Amendment "is a product of the totality of circumstances in which we find ourselves in history."1 He added: "This is fact. What I viewed as reasonableness on the night of September 10th, [2001], I viewed in a very different light on the afternoon of September 11th at the National Security Agency and I actually started to do different things. And I didn't need to ask another 'May I' from Congress or anyone else. It was within my charter."2 The idea of a more secure nation,[3] especially in such a volatile and uncertain world, is appealing to most people. This appeal is particularly strong in times of war and regional instability.[4] Secrecy often accompanies national security, including cybersurveillance, and goes hand in hand with its general cloak of invisibility. People often do not know cybersurveillance is being conducted or that information is being gathered, stored and used against them. The secrecy can be so great that even within the government, some branches might not know about the surveillance being conducted by other branches.[5]

But, like some prescription drugs, secrecy can have significant side effects. What is secret cannot be checked; without proper checking, the government becomes unbalanced. Regardless of how beneficent the government's objectives might be, a secret government does not align with democratic principles and worse, erodes the confidence in government when details emerge.

Secrecy, although intended as a means to an end, can become an end in itself, breeding further unaccountability. It diminishes the

1 General Michael Haydon (ret.), *Keynote Address at the Washington & Lee Cybersurveillance Law Symposium* (Jan. 23, 2015), available at:
https://www.youtube.com/watch?v=VUEuWiXMkBA

2 General Michael Haydon (ret.), *Keynote Address at the Washington & Lee Cybersurveillance Law Symposium* (Jan. 23, 2015), available at:
https://www.youtube.com/watch?v=VUEuWiXMkBA

3 Increased security, though, is often viewed as antithetical to more privacy, as if one is opposed to the other.

4 General Hayden added, "A significant fraction of our population says, 'Why weren't you tracking those guys (the Tsaernav brothers accused of the Boston Marathon bombing) on the Web?'" *Id.*

5 *See*, e.g., Brian Fung, *NSA Refuses to Deny Spying on Members of Congress*, WASH. POST, Jan. 4, 2014, http://www.washingtonpost.com/blogs/the-switch/wp/2014/01/04/the-nsa-refuses-to-deny-spying-on-members-of-congress/.

deep structure of the Constitution's separation of powers, which ensures accountability through interdependence. If disputes between branches occur, most can be resolved within the accepted process of the judicial system. Even if the judicial system plays a role, it can become less effective without a check by the public. As has become apparent with the Foreign Intelligence Surveillance Court and the legislation that spawned it, secret judicial proceedings have significant implications as well. [6]

This paper argues that national security cybersurveillance efforts will be better served by increased transparency, not less, and that such transparency, is required by the deep structure of checks and balances embedded in the Constitution. The deep structures can be found in the separation of powers and several amendments, including the Third, Fourth, Fifth and Fourteenth Amendments.

Separation of powers creates a pervasive system of checks and balances, such as when making laws, war, or treaties, and in appointing officials or judges. This interdependence of branches creates a cooperative process focused on protecting liberty.[7] The Third Amendment limits a certain type of military action in the civilian sphere, the Fourth Amendment prohibits unreasonable searches and seizures, creating a wall of privacy against the government. [8] The Fifth and Fourteenth Amendments provide for due process of law, if the government takes a liberty or property interest.

The importance of constitutional scrutiny as a way to check the actions of another branch cannot be understated. America's Constitution depends on its deep structures, especially the separation of powers and its protection of liberty in its amendments. Its brilliance lies in the way it forces cooperative competence for the government to function. Instead of viewing freedom as contrary to security, it views the two as in alignment – which should give anyone pause that the presumptive good faith of the government behind closed digital doors can substitute for true checks and balances.[9]

---

[6] Diane Carraway Piette & Jesselyn Radack, *Piercing the "Historical Mists": The People and Events Behind the Passage of FISA and the Creation of the "Wall"*, 17 STAN. L. & POL'Y REV. 437 (2006).

[7] An important liberty is the privacy found in the Fourth – and Third – amendments. The government's collection, storage, and use of intimate, personal data can be seen as a significant infringement on privacy, whether privacy is defined as autonomy, freedom of disclosure, freedom from being "seen" or some other formulation.

[8] The Fourth Amendment is a locus of a right to privacy. The evolving conceptualization of privacy, whether it is framed in terms of autonomy, non-disclosure, or non-consensual sharing, is implicated by government snooping, whether the data is actually used or not. For many people, personal information, such as health, wealth and relationship data, is more valuable than material things.

[9] The constitutional requirements are complemented by the utilitarian benefits of outside inspection. While proponents of secrecy often use it as a proxy for efficacy of government, there has been no showing that some checks and balances will not in fact improve the outcome; this, after all, is not only the foundation of the separation of powers, but also the adversary system, where truth will emerge from cross examination and close scrutiny.

§ 1 – BACKGROUND

A) Security and Secrecy

A primary function of the government is to provide security to its people. This function, however, creates tensions in a democratic society regarding the methods used and the scope of permissible security. The tension is often framed as a clash between the values of security versus privacy. Similarly, security is often framed as defensive and protective, not as offensive or intrusive. The motto of the NSA, for example, is "Defending our nation. Serving the future. For the good of the nation, it is imperative that NSA/CSS maintain its cryptologic superiority."[10] These frames are not necessarily accurate or appropriate.

Surveillance has been a part of security for ages, and not only in the United States. For example, the French established Watch Committees in 1792 during the French Revolution.[11] The following year, in 1793, the Law of Suspects was passed, permitting the compilation of lists of suspects.[12] That law played a significant role in domestic surveillance during the Revolution.[13] In the United States, Abraham Lincoln and the Confederate forces instituted domestic surveillance against each other.[14] In World War I, a Military Intelligence Division was created to engage in surveillance. Before World War II, the Federal Bureau of investigation was formed and surveillance was expanded.

In essence, the expansion of surveillance is not a recent phenomenon; it has occurred in many places and throughout the ages. In one historical illustration after another, surveillance was the first step on the road to identifying and gathering suspects, and then arresting and detaining them. While surveillance is not seemingly dangerous in and of itself, it often leads to more dangerous and expansive governmental power.

B) Cybersurveillance

Surveillance today is qualitatively different than old-fashioned pre-digital surveillance. Cybersurveillance need not occur through government agents lurking in shadows, stakeouts, or tailing operations. In fact, there are at least three major differences between cybersurveillance and pre-digital surveillance that require courts to pay careful attention to modern surveillance techniques. One major difference is the reduced transaction costs associated

---

[10] *See* NSA, https://www.nsa.gov/ (last visited March 25, 2015).

[11] Paul R. Hanson, THE HISTORICAL DICTIONARY OF THE FRENCH REVOLUTION 77 (2nd ed. 2015), available at: https://books.google.fr/books?id=mOJdBgAAQBAJ&pg=PA77&dpg=PA77&dq=committee+of+surveillance+french+revolution&source=bl&ots=E3WszEIgJj&sig=ZhCuBcZTvivPsd-9Lxd0LOq8VIw&hl=en&sa=X&ei=i538VPfAC4SMaJHOgaAO&ved=0CEUQ6AEwBA#v=onepage&q=committee%20of%20surveillance%20french%20revolution&f=false.

[12] *Id.*

[13] *Id.*

[14] *See*, e.g., *Spying In the Civil War*, HISTORY.COM: http://www.history.com/topics/american-civil-war/civil-war-spies.

with cybersurveillance, as the person-power required to store data decreases. While cybersurveillance can require costly computer hardware and software, other costs have virtually disappeared.
Second, there is a lack of experience with the level of intrusiveness associated with cybersurveillance that marginalizes its apparent harm.[15] In stakeouts, there is a real person listening or observing in real-time. Phone taps sometimes leave clicks or noises. Even drones can be heard and seen. Cybersurveillance, by contrast, involves computer and cell phone screens, invisible to most, but functioning as a permanent uninvited appendage affixed to devices.
Third, there are multiple sources of cybersurveillance. Each source is capable of providing mountains of data – terabytes really – even information of an intimate and comprehensive nature. The range of data includes governmentally accessed information, information indirectly gathered through private company conduits, and information gathered by individuals through the Internet of Things, multifunctional devices connected to each other and the Internet.

1) Direct Government Cybersurveillance

Multiple government agencies are involved in direct cybersurveillance. These agencies include the NSA, CIA, FBI, and some branches of the military.[16] The government has numerous programs that surveil Americans, both domestically and internationally. For example, a top secret NSA program, "Highlander," tapped into satellite phone transmissions on a Middle Eastern Inmarsat network.[17] The top-secret NSA program PRISM gives the NSA direct access to nine of the largest Internet companies.[18] The FBI has developed "a system of computers and software that completely fuses the FBI's wiretapping outposts with the nation's voice communications network—landlines, cell phones, VOIP services, you name it. Every phone in America is

[15] In the BOURNE SUPREMACY (Universal Pictures 2004), there is a scene where the Jason Bourne is talking on the phone with Pamela Landy, the CIA operative, in NYC. At the end of the conversation, Bourne tells her she should get some sleep because she looks tired. Her look of being spied on says it all — she feels violated.

[16] "Along with the NSA, the Central Intelligence Agency, the Federal Bureau of Investigation and branches of the U.S. military have agreements with such companies to gather data that might seem innocuous but could be highly useful in the hands of U.S. intelligence or cyber warfare units, according to the people, who have either worked for the government or are in companies that have these accords." Michael Riley, *U.S. Agencies Said to Swap Data With Thousands of Firms*, BLOOMBERGBUSINESS (June 15, 2013): http://www.bloomberg.com/news/articles/2013-06-14/u-s-agencies-said-to-swap-data-with-thousands-of-firms.

[17] *See*, e.g., Jonathan D. Forgang, "The right of the People": The NSA, The FISA Amendments Act of 2008, and Foreign Intelligence Surveillance of Americans Overseas, 78 FORDHAM L. REV. 217 (2009), available at: http://ir.lawnet.fordham.edu/flr/vol78/iss1/6;

[18] Elias Groll, *By the Numbers: The NSA's Super-Secret Spy Program, PRISM*, FP PASSPORT (June 7, 2013 12:00 AM), http://foreignpolicy.com/2013/06/07/by-the-numbers-the-nsas-super-secret-spy-program-prism/.

available to them like URLs in a browser. They type it, click it, and they're instantly listening."[19]

Agencies also are developing biometric software programs.[20] The programs include facial recognition software. The Biometric Optical Surveillance System (BOSS)[21] has been tested, even if it is not yet fully operational.

The government uses other cyber methods to obtain information as new technologies continue to emerge. The agencies leverage weak encryption on software to enter the 'backdoors' of private company software and track individuals.[22] Governments sometimes use imitations of cell phone towers, called Stingrays, to gather the numbers of all cell phones within range. The government utilizes "Big Data"[23] methods to analyze the information obtained. It is not a threadbare operation; the NSA, for example, has more than 35,000 employees.[24]

2) Indirect Government Tracking – Leveraging the Actions of Private Companies

Tracking today often originates outside of the government. It results from the efforts of private technology or retail companies, as well as our own efforts to self-surveill every aspect of our lives. Given the range of sources collecting information, governmental collection, storage and analysis of data can seem almost incidental. Indeed, much of the bulk collection of information is not effectuated directly by the government, but rather by private companies.[25] However, the government uses the data stored by telecommunications companies to augment the data it collects through its own agencies.[26]

---

[19] Dan Seitz, *6 New Spy Technologies You Literally Can't Hide From*, CRACKED (September 20, 2010): http://www.cracked.com/article_18771_6-new-spy-technologies-you-literally-cant-hide-from.html.

[20] Cecilla Kang, *Privacy Groups Urge Investigation of Facebook Facial Recognition Tool*, WASH. POST, June 13, 2011: http://www.washingtonpost.com/blogs/post-tech/post/privacy-group-urges-investigation-of-facebook-facial-recognition-tool/2011/06/13/AGSUQCTH_blog.html.

[21] Charlie Savage, *Facial Scanning Is Making Gains in Surveillance,* N.Y. TIMES, Aug. 21, 2013: http://www.nytimes.com/2013/08/21/us/facial-scanning-is-making-gains-in-surveillance.html?pagewanted=all.

[22] Scott Shane, *No Morsel Too Miniscule for All-Consuming NSA*, N.Y. TIMES, Nov. 2, 2013: http://www.nytimes.com/2013/11/03/world/no-morsel-too-minuscule-for-all-consuming-nsa.html.

[23] *See,* e.g., Quentin Hardy, *Big Data's Little Brother*, N.Y. TIMES, Nov. 12, 2013, at B1 ("Collecting data from all sorts of odd places and analyzing it much faster than was possible even a couple of years ago has become one of the hottest areas of the technology industry… Now Big Data is becoming more 'hyper' and including all sorts of sources.").

[24] Scott Shane, *No Morsel Too Miniscule for All-Consuming NSA*, N.Y. TIMES, Nov. 2, 2013: http://www.nytimes.com/2013/11/03/world/no-morsel-too-minuscule-for-all-consuming-nsa.html.

[25] Telephony companies collect great quantity of data, especially involving cell phone location.

[26] *See*, *supra*, Note 24 at A3.

Companies began working with the government on surveillance matters as far back as the Cold War.[27] At that time, the companies helped the government crack secret codes and was premised upon "mutual interests."[28] That mutuality has continued to the present day:

> Thousands of technology, finance and manufacturing companies are working closely with U.S. national security agencies, providing sensitive information and in return receiving benefits that include access to classified intelligence… These programs, whose participants are known as trusted partners, extend far beyond what was revealed by Edward Snowden, a computer technician who did work for the National Security Agency.[29]

While much of the publicity about private-government partnering centered on the telecommunications companies, other types of companies are involved as well:

Makers of hardware and software, banks, Internet security providers, satellite telecommunications companies and many other companies also participate in the government programs. In some cases, the information gathered may be used not just to defend the nation but also to help infiltrate computers of its adversaries.[30]

The leveraging of private efforts creates efficiencies and synergies for the government, and sometimes for the private companies as well. The public first became aware of the extent of the relationships between government and private business after leaks, such as the Snowden revelations.[31]

The partnerships have manifested themselves in different ways. For example, some companies include weak encryption[32] in their software products that the government can easily break.[33] By leaving in such "back doors," and allowing the government to stockpile "zero-day flaws," meaning flaws in software for offensive or defensive government use, the government security agencies accumulate far greater quantities of data. Since technology

---

[27] David Sanger & Nicole Perlroth, *Obama Heads to Security Talks Amid Tensions*, N.Y. TIMES, Feb. 13, 2014, at A1, 3.

[28] *Id.* A1, 3.

[29] Michael Riley, *U.S. Agencies Said to Swap Data With Thousands of Firms*, BLOOMBERGBUSINESS (June 15, 2013):
http://www.bloomberg.com/news/articles/2013-06-14/u-s-agencies-said-to-swap-data-with-thousands-of-firms

[30] *Id.* Michael Riley, *U.S. Agencies Said to Swap Data With Thousands of Firms*, BLOOMBERGBUSINESS (June 15, 2013):
http://www.bloomberg.com/news/articles/2013-06-14/u-s-agencies-said-to-swap-data-with-thousands-of-firms.

[31] The role of private companies has come under intense scrutiny since his disclosure this month that the NSA is collecting millions of U.S. residents' telephone records and the computer communications of foreigners from Google Inc. and other Internet companies under court order.

[32] Encryption is one of the primary defensive tactics to prevent access to and gathering of private information. It is designed to prevent third-parties from accessing the computer through back-doors, but these safeguards are not impregnable and are even are sometimes intentionally weak, making it easier to breach. Information on a site is can be readily downloaded surreptitiously with Web crawlers and other tools.

[33] *Id.* at A3.

companies hold the keys to their software, the government agencies can obtain the keys from them.

These government-private entity partnerships are under reexamination now. Companies have realized, as has the population at large after the Snowden leaks, that governmental requests for information constitute "an intrusion into the privacy of their customers and a risk to their businesses."[34]

3) Indirect Government Cybersurveillance – Companies tracking Individuals

The government-private partnerships are significant mostly because of the large quantities of data obtained by private companies that track individuals. Much of this tracking is legitimized by what will be referred to in this paper as "soft consent" – the implicit acquiescence by Web users of data access, gathering, use and even transfer by technology. In an interconnected world, just about everything we do, from personal hygiene, to finance, to at-home free-time preferences, is observable on the 'grid' since we are connected to others in one or more ways and they track us with our implicit assent. For people to make appointments with doctors, utilize on-line banking privileges, or follow friends on Facebook, they must acquiesce to the disclosure policies of Web sites – policies that often are filled with fine print and run on for paragraphs, if not pages.

Private companies already employ sophisticated facial recognition software programs.[35] Thus, any photos displayed on Instagram, Facebook or other sites can be quickly accessed and matched by the government with its own photo database that includes driver's license and other sources.

Private companies often track people through the Internet using "cookies" which constitute a form of identification tag that companies attach to private computers through Web browsers when an individual uses a computer to visit a Web site. Sometimes, third parties place cookies or tags as well; these are often placed by advertisers with banners or ads from sites that are visited. Individuals can remove cookies or block tracking, but unless a user acts with intentionality – and understands the nature of these invisible trackers – individuals will be subject to multiple cookies that transmit information about them to others. The third-parties who obtain this information, or who place what is known as third-party cookies on computers, generally lurk in the shadows unseen. As one commentator noted:

It's no secret that we're monitored continuously on the Internet. Some of the company names you know, such as Google and

---

[34] *Id.* at A3.

[35] Facebook is one of the largest social media companies and has one of the largest photo banks in the world. *See*, e.g., Russell Brandon, *Why Facebook is Beating the FBI at Facial Recognition*, THE VERGE (July 7, 2014): http://www.theverge.com/2014/7/7/5878069/why-facebook-is-beating-the-fbi-at-facial-recognition.

Facebook. Others hide in the background as you move about the Internet. There are browser plugins that show you who is tracking you. One Atlantic editor found 105 companies tracking him during one 36-hour period. Add data from your cell phone (who you talk to, your location), your credit cards (what you buy, from whom you buy it), and the dozens of other times you interact with a computer daily, we live in a surveillance state beyond the dreams of Orwell.[36]
Email is another fertile source of secondary information. The sending and receiving of emails has content, but also creates metadata. ISPs usually store such metadata, which can be transferred or sold. The NSA and other agencies can track the email metadata – where and when the email took place and who were the parties on it – through companies that store it.[37]
Tracking motivated by commercial purposes is regularly used by the retail industry to track current or potential customers, both on the Internet and in person. When customers enter a store, for example, the store can track their physical movements through cell phones and determine their shopping habits, as well as track the floors and departments that customers visit as well as how long and how often they visit. Advertisers, of course, seek information regarding customer habits. Google Plus, for example, is a social network, but it creates a trove of personal information because it aggregates all Google products in one account, including Gmail, Google maps and YouTube. This allows Google to track the habits of customers.[38]
The tracking of customers can occur even outside of stores through unlikely stationary objects. "Smart" garbage cans, for example, costing in excess of $45,000, were placed in a variety of locations during the London Olympics to track traffic passing by the cans.[39] Those cans, called Renew Pods, remained operational for several years after the Olympics, collecting anonymized information about traffic patterns and potential customers.[40]

---

[36] Bruce Schneier, *Do You Want the Government Buying Your Data From Corporations?*, THE ATLANTIC (April 30, 2013):
http://www.theatlantic.com/technology/archive/2013/04/do-you-want-the-government-buying-your-data-from-corporations/275431/

[37] Shane *Scott, Disclosures on NSA, Surveillance Put Awkward Light on Previous Denials*, N.Y. TIMES, June 12, 2013 at A18.

[38] Claire Cain Miller, *The Plus in Google Plus? It Itlance PFor Google,* N.Y. TIMES, Feb. 15, 2014, at 1. Google Plus has 540 million monthly users and even if they do not visit the social network site, their shopping habits for use by advertisers can be tracked.

[39] The Chief Executive Office of Renew described what the cans did: "During our current trials, a limited number of pods have been testing and collecting anonymized aggregated MAC addresses from the street and sending one report every three minutes concerning total footfall data from sites." Rachel Savage, *Snooping Garbage Bins in City of London Ordered to Be Disabled*, BLOOMBERGBUSINESS (Aug. 12, 2013):
http://www.bloomberg.com/news/articles/2013-08-12/snooping-garbage-bins-in-city-of-london-ordered-to-be-disabled, quoting the CEO Kaveh Memari, from the company's web site, http://renewlondon.com/2013/08/official-message-on-renew-orb-from-ceo-kaveh-memari/.

[40] *Id.*

According to one report, the bins tracked passers-by to study their shopping habits.[41]

Companies also began using radio frequency identification technology (RFID) to track items from a considerable distance. This technology involves the implantation of a small chip in an object so it can be monitored at any time. In 2003, for example, Wal-Mart embedded lipstick containers with RFID technology in its Broken Arrow, Oklahoma store.[42] The containers could be tracked from seven hundred miles away by researchers, and included a video monitor of the consumers handling the products.[43]

4) More Indirect Government Tracking – Self-Cybersurveillance and the Internet of Things

One of the driving forces behind the exponential growth of cybersurveillance is the so-called "Internet of Things," where "smart" devices connect to each other and the Internet[44] to provide a multitude of data-driven opportunities. These devices are "smart" in that they can adapt based on input to improve efficiencies. People can use them to remotely unlock the doors to their homes, turn off kitchen appliances, and check the tire pressure in their cars.[45] When a person awakens, there might be a smart thermostat that will automatically set the temperature to reflect the level of activity in the house. A smart meter can track the electricity used by occupants of the home after they arise.[46] The quality of a person's tooth brushing will be tracked by a smart toothbrush. When the cell phone is turned on, if it ever was turned off, it is tracked every 7 seconds to ensure that it has the preferred location for cell tower reception.[47] The smart watch connects the person to the Internet and other devices, as well as tells time. As people see an interesting situation, they might activate the real-time video feature of the smart glasses they are wearing.

---

41 *Id. See* James Vincent, *(Updated) London's bins are tracking your smartphone*, THE INDEPENDENT, (Aug. 9, 2013), http://www.independent.co.uk/life-style/gatdgets-and-tech/news/updated-londons-bins-are-tracking-your-smartphone-8754924.html.

42 Laura Hildner, *Defusing the Threat of RFID: Protecting Consumer Privacy Through Technology-Specific Legislation at the State Level*, 41 HARV. CIV. RTS.-CIV. LIB. L. REV. 134 (2006). The incident became known as the "Broken Arrow Affair." The use of RFID technology has persisted, although it has been controversial.

43 Laura Hildner, *Defusing the Threat of RFID: Protecting Consumer Privacy Through Technology-Specific Legislation at the State Level*, 41 HARV. CIV. RTS.-CIV. LIB. L. REV. 134 (2006).

44 Julianne Pepitone, *Google House: Tech Giant Spends Billions to Get Inside Your Home*, NBC NEWS, Jan. 14, 2014, http://www.nbcnews.com/tech/innovation/google-house-tech-giant-spends-billions-get-inside-your-home-n9246.

45 *Id.*

46 In the early morning, the smart electric meter is tracking electricity consumption, from unusual surges in use to where in the house the source of usage originates. The house smart thermostat can track how much heat or air conditioning is being used, and when the thermostat should be adjusted. When everyone leaves the house, less energy is required and the thermostat can adjust automatically. These patterns can be stored and utilized for future reference. *Id.*

47 This information can provide a daily sustained record of where that cell phone was 24/7, and by inference, its possessor. That information could be obtained by Stingrays as well. A Stingray is a hand-held device that mimics cell phone towers, obtaining the same information. [Stingrays are being used in some situations by police agencies for crime interdiction.]

The information shared with the manufacturers of connected devices is not readily apparent, and often is provided based on the "soft consent" described above. Through this consent, people effectively acquiesce to tracking by third parties and the controllers of sites. However, people do not understand the implications of generating information that can be shared, sold, and collected – permanently. It is one thing to be followed by a marked police car, and quite another to provide the same information and more through data sharing.

§ 2 – The Importance of Constitutional Scrutiny to Cybersurveillance

As a recent report by the independent Privacy and Civil Liberties Oversight Board noted, there has been "equally widespread consensus within and without the government that the system tilts too far in the direction of secrecy."[48] While legislation providing for checks on secrecy is important, and ought to be enacted, the imposition of constitutional scrutiny is required to properly cabin unrestrained government cybersurveillance. The Framers of the Constitution understood this requirement. As Ben Franklin once declared, "those who surrender freedom for security will not have, nor do they deserve, either one."[49]

The deep structures of the Constitution create government accountability and with accountability, some form of review and transparency. These structures, most notably the separation of powers doctrine, are designed to achieve Ben Franklin's dual objectives of freedom and security.

A) The Separation of Powers – A system of Checks and Balances

The separation of powers doctrine does not have an express niche in the Constitution. Yet, its importance is undeniable. Interdependence among the branches can be seen in many places in the Constitution, requiring more than one branch for the completion of many duties. Duality of action is required for the passage of all laws, requiring both Congress and the President to act. Duality is also required for the enactment of treaties, with two-thirds Senate approval required, as well as for appointments of various governmental officials which must be with the advice and consent of the Senate.[50] Finally, duality is required for impeachment, where the House of Representatives impeaches, and the Senate tries the impeachment, with the Chief Justice of the United States Supreme Court presiding over the trial.

---

[48] *Report on the Telephone Records Program Conducted under Section 215 of the USA PATRIOT Act and on the operations of the Foreign Intelligence Surveillance Court*, The Privacy and Civil Liberties Oversight Board, 192 (Jan. 23, 2014).

[49] To see one interpretation of what Franklin really meant with this phrase, *see*, Benjamin Wittes, *What Ben Franklin Really Said*, LAWFARE (July 15, 2011 6:53 AM): http://www.lawfareblog.com/2011/07/what-ben-franklin-really-said/

[50] *See* U.S. Const. art. II, § 2 (2).

Separation of powers can be traced to the Age of Enlightenment and its philosophers, especially Baron de Montesquieu, author of *The Spirit of the Laws*.[51] A primary objective was to blunt unrestrained power. More than that, though, the system of divided powers was part of the Framers' plan to protect individual liberties.[52] The Framers created an inefficient system, but one whose attributes are numerous and which has survived despite centuries of societal change.

The brilliance of the checks and balances system, and the accompanying interdependence, elides a simple rationale of distrust of government. It pushes beyond the mere fact that each branch is elected or that overlapping duties force different factions to engage in a dialogue, if not directly. Just knowing that there will be examination and inspection by another branch of government presumably modifies the behavior of the participants.[53]

B) The Constitutionnal Amendments

The Amendments to the U.S. Constitution further augment the separation of powers structure and directly protect liberty. In particular, the Fourth Amendment protects the people against unreasonable government searches and seizures. The terms "search" and "seizure" are defined by case law, and theoretically limit cybersurveillance in the context of criminal investigations and prosecutions. The seminal case that defines the term "search", *Katz v. United States*[54], contained language that excluded information knowingly exposed to the public from the definition of the term. The idea of "knowingly exposed to the public" includes most of the data generated by devices connected to the Web or each other.

The Third Amendment also creates a limitation on government excess, distinguishing permissible government quartering of troops in civilian areas from military areas.[55] This recognition of two spheres, civilian and military, also limits what the military can do in the civilian realm. The Amendment should have some applicability in the digital age in terms of limiting military cybersurveillance in the civilian sphere.

In addition, the requirement of due process of law, found in the Fifth and Fourteenth Amendments to the U.S. Constitution, provides another limit on cybersurveillance. If cybersurveillance can be regarded as a taking of property or liberty, then due process will apply and likely given citizens an opportunity to be heard

---

[51] By Charles de Secondat, Baron de Montesquieu. This book, a treatise on political theory, was originally published in 1748.

[52] Andrew P. Napolitano, *A legal History of National Security Law*, 8 N.Y.U. J. L. & LIBERTY 396 (2014).

[53] *See*, e.g., the FISA Amendments of 2008, which took away individual oversight of every warrant and instead provided general oversight.

[54] 389 U.S. 347 (1967).

[55] The Third Amendment states: "[N]o Soldier shall, in time of peace be quartered in any house, without the consent of the Owner, nor in time of war, but in a manner to be prescribed by law." U.S. CONST. amend. III. Of course, the relevancy of the Third Amendment to cybersurveillance depends on its interpretation.

before their property is taken. This provision, in particular, can be viewed as antithetical to government secrecy.

§ 3 – CREATING REAL CHECKS AND BALANCES

The application of constitutional checks and balances is but one way of creating incentives to curtail excessive government cybersurveillance. The use of constitutional and legislative[56] incentives can be used to reign in government snooping in an era where few natural checks and balances exist. The government's contrary incentive -- to gather and keep as much information as possible about others -- is great. Self-surveillance through the Internet of Things will continue to grow,[57] as companies continue to assemble and crunch more data in the commercial realm, and the government will be the welcome receptor of growing streams of information, both directly and indirectly.

A predicate assumption underlying the avenues of information gathering is that the information will not be misused or abused. Further, it might be assumed that in desuetude, the information eventually will be abandoned and destroyed. These assumptions, however, are not likely to occur without a framework of incentives, increasing the urgency of the imposition of real checks and balances.

A) Inter-Branch Transparency

To create real checks and balances, the secrecy of cybersurveillance must be balanced against the opportunity for inspection by another branch. These inspections need not extend to every single surveillance activity, but should extend to at least the outline of activities if agencies are to be kept honest in their surveillance activities. NSA tracking, for example, needs structural checking, and should not be checked solely through haphazard information leaks.[58] Otherwise, the spying of government branches will extend, as it apparently did, to the NSA on Congress.[59] The repercussions are great. As one commentator noted about the hostility toward the NSA after the Snowden revelations: "From NSA's point of view, it's a disaster," Mr. Aid said. "Every new disclosure reinforces the notion that the agency needs to be reined in. There are political consequences, and there will be operational consequences."[60]

---

[56] Legislative incentives are not the focus of this paper. Using a combined approach of both constitutional and legislative incentives will likely be more effective, though, and should be part of a blended approach to the problem.

[57] The Internet of Things is expected to become a $10 Trillion.

[58] Shane Scott, *Disclosures on NSA, Surveillance Put Awkward Light on Previous Denials*, N.Y. TIMES, June 12, 2013 at A18.

[59] Brian Fung, *NSA Refuses to Deny Spying on Members of Congress*, WASH. POST, Jan. 4, 2014, http://www.washingtonpost.com/blogs/the-switch/wp/2014/01/04/the-nsa-refuses-to-deny-spying-on-members-of-congress/.

[60] Scott Shane, *No Morsel Too Miniscule for All-Consuming NSA*, N.Y. TIMES, Nov. 2, 2013, http://www.nytimes.com/2013/11/03/world/no-morsel-too-minuscule-for-all-consuming-nsa.html.

Even with inspection, there must be real inspections to be effective. A lack of transparency is evident when considering government attempts to reign in Executive and military surveillance through the Foreign Intelligence Surveillance Act[61] and the creation of the surveillance court.

Also, it is important for consumers to understand the extent that private companies are cooperating with the government – what is happening to information collected and stored by those companies?

B) Open Judicial Review

While it was thought that the FISA court would provide a check on cyber operations, the secrecy of the court, and the lack of a true adversarial process in its processes, has shown to the contrary. For example, of the first 22,987 applications by the government to the court for information, all but five were approved in some form or another.[62]

This record of approval by the FISA court infers deference in the name of national security that is just as dangerous as no scrutiny at all. Because the court exists, some might think that it interposes a real check on power, when it does not. The input and opposition of defense counsel would provide a real check on prosecutorial and governmental power; how that is configured can be determined to best fit the circumstances and the nature of the application is the question. What this need suggests, though, is that the opportunity to be heard, so important to the fundamental notion of due process, is an essential check on government cybersurveillance as well.

C) No Soft Consent

Under the Fourth Amendment consent doctrine,[63] disclosure to third parties has become a death knell to the privacy wall around that information. Thus, when medical information is disclosed to insurers, or phone numbers to the telephone company, the information is considered to be effectively in the public domain. This analysis should not apply in the digital age, where being on the "grid"[64] means the constant communication of information – information generated behind closed doors as well as in front of them. The *Kyllo v. United States*[65] limitation, stopping government from using advanced technology that allows it to effectively peer through walls, as well as off the walls, should be resurrected and enforced.

---

[61] Another way the government obtains information is through warrants and requests under FISA. *See* Foreign Intelligence Surveillance Act, 50 U.S.C. §§ 1801-1885 (2010).

[62] *See*, e.g., Larry Abramson, *We Approve 99 Percent of Wiretap Applications*, NPR ONLINE, THE TWO-WAY, (Oct. 15, 2013 3:57 PM):
http://www.npr.org/blogs/thetwo-way/2013/10/15/234840282/fisa-court-we-approve-99-percent-of-wiretap-applications

[63] *See*, e.g., *Smith v. Maryland*, 442 U.S. 735 (1979).

[64] The "grid" denotes being a part of society. To be unconnected today, and without any digital devices, today either is a conscious choice to be isolated or the product of insufficient resources.

[65] 533 U.S. 27 (2001).

The consent doctrine of different substantive areas is instructive, from the Fifth Amendment understandings of consent under the voluntariness standard of *Miranda v. Arizona*,[66] to the Sixth Amendment approach of *Johnson v. Zerbst*,[67] requiring a knowing and intelligent waiver of a right to counsel. Given the new center of gravity in the digital age, these stronger versions of consent should be imported into the digital consent realm. Otherwise, the notion of consent will be swept away with the flippant changes of privacy policy by a large telecommunications or social media company.

CONCLUSION

Government efforts to maintain national security are rarely transparent, since secrecy is usually the coin of the realm. Secrecy is a means to an important and legitimate end, but it should not become the end itself. Yet, the Constitution does not have an emergency exception, condoning wholesale, unreviewable surveillance, especially when there is no active war. The United States' democracy is built on the deep structures of separation of powers, originating with the Baron de Montesquieu and the philosophers of the Age of Enlightenment, not only because of a strong distrust of government, and was designed to mandate some cooperative competency between branches. National security concerns, however, often elide transparency, especially with respect to cyber surveillance. To comply with constitutional dictates, effective scrutiny must be applied to government cybersurveillance. Scrutiny must include the effective functioning of the separation of powers doctrine, in which one branch checks another, more robust consent requirements, and incentives for curtailment of excessive cybersurveillance. This will help, if not ensure, that the government is using proper means to achieve its valid ends.

[66] 384 U.S. 436 (1966).
[67] 304 U.S. 458 (1938).