# INTERNATIONAL JOURNAL OF **DIGITAL AND DATA LAW**

# REVUE INTERNATIONALE DE DROIT **DES DONNÉES ET DU NUMÉRIQUE**

Vol. 5 - 2019

ISSN 2553-6893

IMODEV
LES ÉDITIONS

International Journal of Digital and Data Law
Revue internationale de droit des données et du numérique

**Direction :**
**Irène Bouhadana & William Gilles**

ISSN : 2553-6893

**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 de droit des données et du numérique (RIDDN)/ the International Journal of Digital and Data Law** 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. Enfin, elle est avocate au barreau de Paris, associée de BeRecht Avocats.

**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. Fondateur et associé de BeRecht Avocats, il aussi avocat au barreau de Paris et médiateur professionnel agréé par le CNMA.

**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 Digital and Data Law / Revue Internationale de droit des données et du numérique (RIDDN)** 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. She is an attorney at law at the Paris Bar and a partner of BeRecht Avocats.

**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. Founder and partner at BeRecht Avocats, he is an attorney at law at the Paris Bar and a professional mediator accredited by the CNMA.

**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].

# U.S. CYBERSURVEILLANCE IN THE POST-SNOWDEN ERA

by **Russell L. WEAVER**, Professor of Law & Distinguished University Scholar, University of Louisville, Louis D. Brandeis School of Law (USA). *Professor Weaver gives particular thanks to Dean Colin Crawford's faculty development fund for sponsoring Professor Weaver's participation in this event.*

In 2013, Edward Snowden revealed to the public that the U.S. National Security Agency (NSA) was operating a massive, secret, cybersurveillance operation[1], thereby touching off a national debate regarding the permissibility and desirability of the NSA program[2]. In the ensuing years, both Congress and the American public debated fundamental issues regarding the relationship between the citizen and the government. Entwined up in these debates were issues relating to national security, especially the need to detect and apprehend potential terrorists, against the citizenry's interest in privacy against governmental surveillance and intrusion[3].

Now that five years have passed since the Snowden disclosures, it is appropriate to reflect on how these societal debates have played out. In the interim, much has happened. In addition to the congressional and societal debates regarding whether government should be conducting such an operation, there have been efforts to litigate regarding the permissibility of that program. Further, the U.S. Congress has voted twice on the extent to which governmental cyber-surveillance should be allowed to continue[4]. This article analyzes how Congress and the American people have responded to the Snowden revelations.

---

[1] *See* S. SHANE, "No Morsel Too Minuscule for All-Consuming NSA: From Spying on Leader of U.N. to tracking Drug Deals, on Ethos of 'Why Not?'", *The New York Times*, A10 (Nov. 13, 2013); D. STANGLIN; "Snowden Says NSA Can Tap Email Chats", *The Courier-Journal*, A3 (Aug. 1, 2013).

[2] *See* J. MARKOFF, "The Snowden Effect: 2 Pioneers Debate the Future of the Net", *The Washington Post* 14 (Jan. 2, 2014) ("Edward Snowden's actions have raised a new storm of controversy about the role of the Internet."); J. CALMES & N. WINGFIELD, "Visions Collide as Silicon Valley Leaders Go to White House: Tech Firms Want NSA", *International New York Times* 17 (Dec. 19, 2013); J. RISEN, "Microsoft", *International Herald Tribune* 5 (July 13, 2013).

[3] *Id.*; *see also United States v. Nixon*, 418 U.S. 683 (1974) (ordering President Nixon to release information, but noting that confidentiality regarding the President's conversations and correspondence is generally privileged, and going on to note that this privilege is "fundamental to the operation of Government and inextricably rooted in the separation of powers under the Constitution.").

[4] *See* SCHNEIER, *supra* note ____.

## § 1 – CYBER-SURVEILLANCE AT THE TIME OF THE SNOWDEN REVELATIONS

The program that Snowden revealed was massive. At the time, the NSA had a budget in excess of $10 billion per year[5], as well as 35,000 employees[6], and it was systematically collecting and storing huge amounts of data[7]. Among the data that it was collecting were cell phone call records, e-mails, text messages, credit card purchase records and information derived from social media networks[8]. In total, the NSA had intercepted some 182 million communication records[9]. The overwhelming majority of this cyber-surveillance was being conducted in secret, and the American public was previously unaware of the nature or scope of the NSA's activities.

Even though the NSA's surveillance operation was primarily focused on foreign intelligence targets, it inevitably swept up large numbers of records involving Americans[10]. The NSA claimed that it operation was focus on communications with "foreign intelligence value"[11] and on foreign intelligence targets[12]. Indeed, as President Obama boldly proclaimed, "Nobody is listening to your telephone calls."[13] However, Obama admitted that, when Americans communicate with foreigners, the NSA may be able to target their communications[14]. Since there were literally billions of communications between U.S. citizens and foreigners per day, Obama's reassurance provided little consolation to the American public.

The other major problem was that the NSA was collecting and storing large quantities of electronic information. In the process, the NSA was deceiving the public by publicly stating that it was not collecting data except under limited circumstances: when it believed that the recording or transcript contained "foreign intelligence information," evidence of a possible crime, a "threat of serious harm to life or property," or that shed "light on technical issues like encryption or vulnerability to cyber attacks."[15] The reality was quite different. Taking advantage of the digital capacity to easily store large quantities of information, the NSA had established a data storage center which allowed it to collect, store

5 *See id.*

6 *See id.*

7 *See* M. MENDOZA, "Reagan's Order Led to NSA's Broader Spying", *The Courier-Journal*, A10, c. 1-6 (Nov. 24, 2013).

8 *See id.*; *see also* P. MAASS, "How Laura Poitras Helped Snowden Spill His Secrets", *The New York Times*, § MM (Aug. 13, 2013); Ch. SAVAGE, "C.I.A. Ties to AT&T's Add Another Side to Spy Debate", *International Herald Tribune*, A5 (Nov. 8, 2013).

9 *See* M. MENDOZA, "Reagan's Order Led to NSA's Broader Spying", *The Courier-Journal*, A10, c. 1-6 (Nov. 24, 2013).

10 *See* P. SEMANSKY, "NSA Ends Sept. 11-Era Surveillance Program", *The Two Way*, National Public Radio (Nov. 29, 2015).

11 *See* S. SHANE, "Documents Detail Restrictions on N.S.A. Surveillance", *The New York Times* A9 (June 21, 2014); *see also* MENDOZA, *supra* note 8.

12 *See* SHANE, *supra* note 9.

13 *See id.*

14 *See* K. JOHNSON, "NSA: Surveillance Foiled 50 Terrorist Plots; Director Says NYSE Was Among Targets", *USA Today*, 5A (June 20, 2013).

15 *Id.*

and search huge quantities of information[16], and allowed it to routinely collect extraordinarily large amounts of information regarding virtually everyone[17].

The NSA's governing legal structure is the Foreign Intelligence Security Act of 1978 (FISA)[18], which was originally conceived of as a way to respond to "foreign powers" or "agents of foreign powers" who are suspected of engaging in espionage or terrorism[19]. The term "foreign powers" was defined to focus on "groups" engaged in international terrorism[20]. However, the concept was later expanded to include so-called "lone wolfs" – a person who is engaging in or preparing for terrorist acts who does not have a connection to a foreign government or a terrorist group[21].

The Protect America Act of 2007 provided that communications that begin or end in a foreign country can be wiretapped without FISA supervision[22]. FISA also created the Federal Intelligence Surveillance Court (FICSC), and authorized it to issue surveillance warrants against foreign intelligence agents working inside the U.S. Warrants are issued ex parte, in secret, without adversarial proceedings, and the records of the proceedings are withheld from the public.

It is not clear how rigorously the FISC reviewed warrant applications. Over the years, FISC has issued tens of thousands of FISA warrants, and only denied a handful of requests. Those denials were appealable to the United States Foreign Intelligence Surveillance Court of Review, which also functioned in secret, but there have been few appeals[23].

Under pre-existing law, the NSA was allowed to eavesdrop on communications cables outside the U.S., as well as communications cables between foreign countries that passed through the U.S.[24]. FISA, Section 702, expanded the NSA's authority by allowing the NSA to tap cables passing through the U.S., and by giving it the right to collect data directly from internet companies through a program called PRISM[25]. Although these programs were focused on collecting data regarding non-Americans, communications by Americans were inevitably swept up in the process[26].

16 *See* S. SHANE & D. E. SANGER, "Job Title Key to Inner Access Held by Leaker", *The New York Times* A1 (July 1, 2013).
17 *See* Shane, *supra* note 9.
18 50 U.S.C. § 1801 *et seq.*
19 *Id.*
20 *Id.* at § 1801(a) (4) & (5).
21 50 U.S.C. § 1801(b)(1)(C).
22 Pub. L. 110-55.
23 50 U.S.C. § 105(a)(3) & (b).
24 *Id.*
25 *Id.*
26 *Id.*

## § 2 – POST-SNOWDEN ALTERATIONS TO THE U.S. CYBERSURVEILLANCE PROGRAM

Post-Snowden, have there been significant changes in the way that the NSA has functioned? While there have been changes, the alterations are perhaps not as dramatic as one might have anticipated. In the aftermath, Section 702 of FISA has not only survived, but was re-enacted during the Obama administration and the Trump administration[27]. The most recent re-enactment occurred in January, 2018[28]. Although these re-enactments were opposed by privacy advocates, and championed by national security hawks, the Trump era re-enactment passed easily (65 - 34 in the U.S. Senate)[29]. Privacy advocates did succeed in imposing certain limitations, but failed in their efforts to promote other limitations[30].

The re-enactments limited NSA's cybersurveillance authority in important respects. For one thing, Congress limited the NSA's authority to engage in the bulk collection of metadata from Americans' phone calls[31]. Under the program, as it existed before the Snowden revelations, large telecom companies were required to hand over "metadata" (e.g., information regarding phone numbers and the duration of calls) to the NSA, but were not required to turn over the content of phone conversations. Nevertheless, the NSA was bulk collecting information from providers such as Verizon[32]. And, of course, the worry was that the NSA might indiscriminately search through the bulk collection. Although the 2015 law allowed the NSA to continue accessing metadata[33], the law provided that the data would remain with the telecom service providers rather than being collected and stored by the NSA[34]. In order to gain access to such information, the NSA was required to seek a court order giving it access to specific records[35].

The NSA was also authorized to engage in surveillance regarding so-called "upstream" collections of information from telecommunications companies like AT&T and Verizon[36]. In other words, the NSA collected emails and texts that crossed U.S. borders, including messages that mentioned identifying terms (e.g., email addresses) related to "foreigners who the agency was spying on even though the messages were not to or from those targets."[37]

---

27 *See* SCHNEIER, *supra* note ____.

28 *Id.*

29 *See* K. DEMIRJIAN, 'Senate Passes Bill to Extend Key Surveillance Program, Sending It to Trumps Desk", *The Washington Post* (Jan. 18, 2018).

30 *See House Votes to Renew Surveillance Law, Rejects Privacy Limits; Intelligence Agencies, Trump Scores a Victory, Boston Globe* A (Jan. 12, 2018).

31 *See* P. SEMANSKY, "NSA Ends Sept. 11-Era Surveillance Program", *The Two Way*, National Public Radio (Nov. 29, 2015).

32 *Id.*

33 *Id.*

34 *Id.*

35 *Id.*

36 Ch. SAVAGE, "N.S.A. Halts Collection of Americans' Emails About Foreign Targets", *New York Times* (Apr. 28, 2017).

37 *Id.*

Before Snowden's revelations, the NSA's collection of this information was permitted under the FISA Amendments Act of 2008, but was largely unknown by the American public[38], and the government took steps to convince the courts that these upstream communications were permissible under the U.S. Constitution and statutory requirements, and that such "about" communications were an important tool in fighting terrorism: "Under the proposed method of conducting electronic surveillance, then, N.S.A. will be in a position not only to learn information about the activities of its targets, but also to discover information about new potential targets that it may never have otherwise acquired."[39] Of course, one of the problems with this "about" collection system was that it snagged "tens of thousands of purely domestic emails each year."[40] Despite the firestorm of controversy raised by the Snowden revelations, Congress chose not to end the upstream program in its 2015 re-authorization[41]. However, in 2017, the program was terminated in 2017 by the NSA rather than by Congress, following the FISA court's conclusion that it was being conducted unconstitutionally[42]. The problem was that the collection program had been used to gather information about Americans when the NSA was not supposed to have been searching for information related to Americans[43]. Voluntarily, the NSA chose to limit its collection of upstream internet messages to those that are sent directly to or from foreign intelligence targets, forgoing collection of messages that simply reference those targets[44].

The 2015 amendments also did not prohibit the NSA's so-called PRISM program, a so-called "downstream" method of collecting information sent over the internet. Under the PRISM program, the NSA was able to gain direct access to the servers of online providers such as Google, Facebook, Microsoft and Yahoo[45]. However, the PRISM system does not collect "about" communications[46]. The official said the intelligence court's presiding judge, Judge Rosemary M. Collyer, has now authorized the agency to use Americans' identifiers to query the newly captured upstream internet messages, too, for future intelligence investigations. Privacy advocates refer to this practice as the "backdoor search loophole" and want Congress to require the government to obtain a warrant to search for Americans' incidentally collected information within the warrantless surveillance repository[47].

---

38 *Id.*
39 *Id.*
40 *Id.*
41 *Id.*
42 *Id.*
43 *Id.* (SAVAGE)
44 *Id.*
45 *See* T. B. LEE, "Here's Everything We Know About PRISM to Date, Workblog", *The Washington Post* (June 12, 2013).
46 *Id.*
47 *Id.*

The 2018 re-enactment did make one significant change regarding the use of surveillance data. One problem with Section 702 was that, although federal law enforcement agents were allowed to examine databases related to foreign targets, there was a risk that the NSA would use this information to obtain information about Americans who have corresponded with those foreign targets[48]. Under the re-enactment, although the NSA was allowed to continue viewing surveillance data related to Americans without a court order, provided that the data relates to counter terrorism, counterintelligence or counterespionage, they were not free to use that information in ordinary criminal cases without first obtaining judicial approval[49].

## CONCLUSION

The Snowden revelations touched off a fire-storm of controversy regarding governmental cybersurveillance operations. In the U.S., although the surveillance operation continues, it has been curtailed somewhat. The U.S. government no longer bulk collects and stores millions of items of information. But it's secret surveillance operation, and many of its components, continue.

Despite the changes that occurred in the post-Snowden era, governmental cyber-surveillance remains a significant issue. For example, in 2017, WikiLeaks broke another story showing that governmental cyber-surveillance continues[50]. In particular WikiLeaks revealed that the U.S. government has developed an array of mechanisms that allow it to break into "Apple and Android smart phones," as well as "Windows computers, automotive computer systems, and even smart televisions."[51] Apparently, there were at least 14 flaws in Apple's operating system for phones and tablets, and two dozen flaws in the Android system, and these flaws could leave individual phones vulnerable to being snooped on[52]. While these flaws did not enable the government to gather information en masse, they did enable the government to pry into individual phones, computers and smart televisions[53].

48 *See* DEMERJIAN, *supra* note ____.

49 *See id.*

50 *See* V. GOEL & N. WINGFIELD, "WikiLeaks Reignites Tensions Between Silicon Valley and Spy Agencies", *International New York Times* A 10 (Mar. 7, 2017).

51 *Id.*

52 *Id.*

53 *Id.*