The State of French Surveillance Law

by

Bénédicte Dambrine

22 December 2015

Contents

Introduction 2

Law n°2015-912 of 24 July 2015 4

SCOPE OF THE LAW 4

WHAT ARE THE DIFFERENT TECHNIQUES FOR INTELLIGENCE GATHERING? 5

PROCEDURE 6

MEASURES FOR INTERNATIONAL INTELLIGENCE OPERATIONS 6

DATA RETENTION 7

RECOURSE FOR INDIVIDUALS 7

OBLIGATIONS ON TELECOM OPERATORS AND HOSTING PROVIDERS 7

REMARKS 8

Recent Developments 8

Introduction

In a historic decision rendered on October 6, 2015, the Court of Justice of the European Union (CJEU) took down Safe Harbor, the agreement entered into by the United States and the European Union in 2000 that allowed for consumer data to be transferred from the European Union to the United States.[1] Since it came into force, Safe Harbor has been used by more than 5000 companies as a legal basis for data transfers. All these companies are now scrambling to find alternative options to continue data flows between the US and Europe.

The underlying reason for the Court to strike down Safe Harbor was its view of US surveillance practices. Indeed, after Edward Snowden's staggering revelations on 6 June 2013, the world discovered the scope and extent to which the National Security Agency (NSA) was collecting personal data about individuals - including Europeans - from private entities.[2]

Even though the Court recognizes in its judgment that some derogations may exist for national security necessities, it explains that protection of the fundamental right to respect for private life at EU level requires derogations and limitations in relation to the protection of personal data to apply in so far as strictly necessary."[3] The Court notes that "the United States authorities were able to access the personal data transferred from the Member States to the United States and process it in a way incompatible, in particular, with the purposes for which it was transferred, beyond what was strictly necessary and proportionate to the protection of national security."[4] According to the Court, US legislation "authorizes, on a generalized basis, storage of all the personal data of all the persons whose data has been transferred from the European Union to the United States without any differentiation, limitation or exception being made in the light of the objective pursued and without any objective criterion being laid down by which to determine the limits of the access of the public authorities to the data, and of its subsequent use, for purposes which are specific, strictly restricted and capable of justifying the interference which both access to that data and its use entail."[5] The Court references to the communication issued by the Commission on 27 November 2013[6], in which the Commission states that "all companies involved in the PRISM programme [a large-scale intelligence collection programme], and which grant access to US authorities to data stored and processed in the [United States], appear to be Safe Harbor certified' and that '[t]his has made the Safe Harbor scheme one of the conduits through

[1] CJEU – Case-362/14, 6 October 2015 (available at http://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d2dc30dddc85f97be12d47869df0aee39acfda80.e34KaxiLc3qMb40Rch0SaxuRbN90?text=&docid=169195&pageIndex=0&doclang=en&mode=req&dir=&occ=first&part=1&cid=491649)

[2] http://www.bbc.com/news/world-us-canada-23123964

[3] CJEU – Case-362/14, 6 October 2015 (available at http://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d2dc30dddc85f97be12d47869df0aee39acfda80.e34KaxiLc3qMb40Rch0SaxuRbN90?text=&docid=169195&pageIndex=0&doclang=en&mode=req&dir=&occ=first&part=1&cid=491649)

[4] Id

[5] Id

[6] Communication COM(2013) 847 (available at http://ec.europa.eu/justice/data-protection/files/com_2013_847_en.pdf)

which access is given to US intelligence authorities to collecting personal data initially processed in the [European Union]."

Another major concern that led to this outcome was the Court's view regarding the lack of administrative or judicial means of redress for data subjects to access or, as the case may be, rectify or erase such data.

Pursuant to the Court, "the term 'adequate level of protection' must be understood as requiring the third country in fact to ensure, by reason of its domestic law or its international commitments, a level of protection of fundamental rights and freedoms that is essentially equivalent to that guaranteed within the European Union."

In light of these observations, the Court determined that the US was not providing adequate level of protection, therefore prohibiting forward data transfers from Europe to the United States on the basis of Safe Harbor.

Some critics deplored the decision and contended that the analysis of the PRISM program made by the Court was erroneous, adding that the latter failed to take into account the recent legislative changes such as the US Freedom Act amending the controversial US Patriot Act.[7]

In this context, Professor Peter Swire and the Future of Privacy Forum released a report on December 17, 2015 titled "U.S. Surveillance Law, Safe Harbor, and Reforms Since 2013."[8]

The study addresses serious misunderstandings of U.S. national security laws and covers three critical areas: (1) the fundamental equivalence of the United States and EU member States as constitutional democracies, (2) the Section 702 PRISM and Upstream programs are reasonable and lawful responses to changing technology, and (3) the U.S. Congress and executive branch have instituted over two dozen significant reforms to surveillance law and practice since 2013.[9]

At the same time, Europe has been facing several terrorist attacks for the past few years. Back in 2012, France went through a terror period when Mohamed Merah, during the course of several months, attacked a Jewish school and murdered several members of the military.[10] More recently, in August 2015, an attack in the Thalys train could have led to the death of numerous people had the perpetrator not been cut short by American tourists present in the train when the attack occurred.[11]

---

[7] IAPP audio recording – A future with no US-EU Safe Harbor (available at https://iapp.org/news/a/with-safe-harbor-invalid-whats-next-for-privacy-pros/)
See also https://iapp.org/news/a/solving-the-unsolvable-on-safe-harbor-the-role-of-independent-dpas *and before the decision* https://iapp.org/news/a/dont-strike-down-the-safe-harbor-based-on-inaccurate-views-on-u-s-intelligence-law/

[8] Report available at https://fpf.org/wp-content/uploads/2015/12/White-Paper-Swire-US-EU-Surveillance.pdf

[9] https://fpf.org/2015/12/17/new-swire-fpf-report-u-s-surveillance-law-safe-harbor-and-reforms-since-2013/

[10] http://www.huffingtonpost.com/2012/03/22/toulouse-shooting-mohamed-merah-shot-dead_n_1372387.html

[11] http://www.theguardian.com/world/2015/aug/22/europe-high-alert-french-train-attack

Early this year, two radical Islamic gunmen targeted the offices of the satirical newspaper Charlie Hebdo in Paris, causing twelve people to die. A few days later, an accomplice took several people hostage at a kosher supermarket and killed four of them.[12] In the midst of these security crisis, the French government reacted by proposing a bill on mass surveillance a few months later. After the *Conseil Constitutionnel* invalidated some parts, the law was passed on 24 July 2015 and entered into effect on 26 July 2015.[13] The law received tremendous backlash from civil liberties groups and privacy advocates. Amnesty International warned of "extremely large and intrusive powers" without judicial control.[14]

This white paper examines the most recent surveillance law in France with a view to offering a clear understanding of France's current surveillance practices. National security and mass surveillance programs have been and will always be of the utmost importance for sovereign states. They are becoming more and more crucial as attacks against Western nations from terrorists of all parts of the world have never been so big, both quantitatively and with respect to the means and level of technicality at stake. But, the compatibility of these programs with values and principles of modern democracies and fundamental rights are likely to be increasingly challenged. In this context, this paper aims to provide clarification regarding France's surveillance legal framework, particularly the process, authorities involved and types of redress available.

Law n°2015-912 of 24 July 2015

The law aims to provide France with a single legal framework for its intelligence gathering activities, by defining applicable principles, defining the different techniques that are used and by reinforcing control.[15] The goal is to strengthen protection of individual liberties while securing the action of specialized services.[16] The law is now codified in *Livre VIII* of the French Internal Security Code entitled "Intelligence".[17]

SCOPE OF THE LAW

Documentation and preparatory legislative work issued by the government, governmental agencies explain that surveillance practices can only be exercised for enumerated and limited purposes, allowing balance between security and privacy rights.[18] French intelligence public policy contributes to the

[12] http://www.bbc.com/news/world-europe-30708237
[13] Law n° 2015-912 of 24 July 2015 related to intelligence (available at http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000030931899&categorieLien=id)
[14] http://www.theguardian.com/world/2015/may/05/france-passes-new-surveillance-law-in-wake-of-charlie-hebdo-attack
[15] Law n° 2015-912 of 24 July 2015 related to intelligence – *Exposé des motifs* (available at http://www.legifrance.gouv.fr/affichLoiPubliee.do;jsessionid=AC82D0703DA2374DEF16BEA404A88989.tpdila23v_3?idDocument=JORFDOLE000030375694&type=expose&typeLoi=&legislature=14)
[16] Id
[17] French Internal Security Code is available at http://www.legifrance.gouv.fr/affichCode.do?cidTexte=LEGITEXT000025503132&dateTexte=20151111
[18] Impact study (*étude d'impact*) of the law (available at file:///C:/Users/FPFBenedicte/Downloads/ei_renseignement_cm_19.03.2015.pdf)

national security strategy and to the defense and promotion of fundamental interests of the Nation.[19] Intelligence services can operate for the following limited purposes:[20]

i. National independence, territory integrity and national defense;
ii. Major foreign policy interests, execution of France's European and international agreements and prevention of any foreign interference;
iii. France's major economic, industrial and scientific interests;
iv. To prevent terrorism;
v. To prevent immediate threats to public order;
vi. To prevent organized crime;
vii. To prevent the proliferation of weapons of mass destruction.

The French Highest Administrative Court (*Conseil d'Etat*) issued an opinion in March 2015 in which it explained that the exhaustive definition of the different purposes for which intelligence techniques are allowed – some of which being very privacy invasive – constitutes the principal safeguard that those techniques will only be employed for legitimate purposes.[21] According to legislative preparatory work documents, individuals' privacy is safeguarded because violations are only allowed for public interest reasons set forth in the law and need to be done in light of the proportionality principle.[22]

WHAT ARE THE DIFFERENT TECHNIQUES FOR INTELLIGENCE GATHERING?

Intelligence agencies, upon proper prior authorization, can collect electronic communications, information or documents processed by telecom operators, including technical data related to connection or subscription identification numbers, location data, duration and time of communications.[23] For prevention of terrorism only, collection from telecom operators and hosting providers of real time traffic data and log data of individuals previously flagged as representing a threat can be authorized.[24] Intelligence agencies can also deploy algorithms to analyze traffic and log data to detect potential terrorist threats and can obtain access to traffic data from telecom operators and to log data kept by hosting providers, including social media services.[25] The most controversial provision relates to the analysis by intelligence agencies of all traffic and log data on an anonymized basis to identify suspicious activity and potential terrorist threats.[26]

[19] Article L. 811-1 of the French Internal Security Code
[20] Article L. 811-3 of the French Internal Security Code
[21] *Conseil d'Etat – séance du jeudi 12 mars 2015 – avis sur un projet de loi relative au renseignement* (available at file:///C:/Users/FPFBenedicte/Downloads/avis_ce_prmx1504410L_cm_19_03_2015.pdf)
[22] Law n° 2015-912 of 24 July 2015 related to intelligence – *Exposé des motifs* (available at http://www.legifrance.gouv.fr/affichLoiPubliee.do;jsessionid=AC82D0703DA2374DEF16BEA404A88989.tpdila23v_3?idDocument=JORFDOLE000030375694&type=expose&typeLoi=&legislature=14)
[23] Article L. 851-1 of the French Internal Security Code
[24] Article L. 851-2 of the French Internal Security Code
[25] Articles L. 851-1 to L. 851-7 of the French Internal Security Code
[26] Article L. 851-3 of the French Internal Security Code

Hogan Lovells attorney Winston Maxwell explained that "to some lawyers, analyzing the traffic and log data of the entire population of France violates the proportionality principle set forth in the European Court of Justice's Digital Rights Ireland Decision".[27]

Other provisions set forth conditions under which can be collected any electronic communications,[28] phone-tapping, confidential communications or wiretapping and images from private spaces and vehicles.[29]

PROCEDURE

Intelligence agencies' operations require an authorization from the Prime minister which is delivered after an opinion from the Commission for Oversight of Intelligence Gathering Techniques (*Commission National de contrôle des techniques de renseignement*) ("CNCTR").[30]However, opinions from the CNCTR are not binding.[31] The authorization is valid for a maximum period of four months.[32]In cases of "absolute emergency" and only for three limited purposes (prevention of terrorism, safeguard of national integrity and territory, and prevention of immediate threats), the Prime minister may deliver an authorization without prior opinion from the CNCTR. The request for authorization must be written and set forth certain details, including the different techniques to be undertaken, the purposes for data collection and the authorization duration. The CNCTR, which is an independent administrative agency (*Autorité Administrative Indépendante*)[33], can issue a recommendation, at any time, for the intelligence techniques to be interrupted and collected data destroyed.[34]It can also refer to the *Conseil d'Etat* as a last recourse.[35]

Because these provisions are considered to be within the scope of "administrative police", they do not require a prior authorization from a judicial judge. However, individuals do have recourse rights *a posteriori*.[36]

MEASURES FOR INTERNATIONAL INTELLIGENCE OPERATIONS

The law originally contained a provision that authorized, for the sole purpose of the protection of the Nation's fundamental interests, surveillance of communications issued or received abroad.[37]

However, this provision was invalidated by the Constitutional Council (*Conseil Constitutionnel*) in a decision dated 23 July 2015.[38] The Constitutional Council argued that the provision failed to describe the

[27] Hogan Lovells blog post – August 6th, 2015 by Winston Maxwell (Available at http://www.hldataprotection.com/2015/08/articles/international-eu-privacy/french-surveillance-law-permits-data-mining-drawing-criticism-from-privacy-advocates/)
[28] Article L. 852-1 of the French Internal Security Code
[29] Articles L. 853-1 to L. 853-3 of the French Internal Security Code
[30] Article L. 821-1 of the French Internal Security Code
[31] Article L. 821-4 of the French Internal Security Code
[32] Article L. 821-4 of the French Internal Security Code
[33] Article L. 831-1 of the French Internal Security Code
[34] Article L. 833-6 of the French Internal Security Code
[35] Article L. 833-8 of the French Internal Security Code
[36] See section "recourse for individuals" below
[37] Former Article L. 854-1 of the French Internal Security Code

conditions under which collected data would be used, kept and deleted; the type of control by the CNCTR; and citizen legal recourse.[39]

DATA RETENTION

Collected data is to be destroyed:[40]

i. 30 days after the day it was collected for data collected about suspected individuals in the circle of the person subject of the authorization or wiretapping data.
ii. 120 days after the day it was collected for private spaces and vehicles wiretapping and certain log data, except for log data collected under the conditions set forth in article L. 851-1 (see iii)
iii. 4 years after the day it was collected for traffic data from telecom operators and log data kept by hosting providers.

For encrypted data, the data retention period starts from the day it is decrypted. However, it cannot be kept more than six years from the day it was collected.

Even though data retention periods have been increased compared to the old law, data collected by intelligence agencies must be destroyed when it is no longer necessary for any of the purposes it was collected.[41]

RECOURSE FOR INDIVIDUALS

Any individual wishing to verify that no intelligence operations is irregularly conducted about himself/herself may refer his/her case to the *Conseil d'Etat*. However, the individual must have first filed a complaint with the CNCTR.[42]

The Constitutional Council invalidated some language of the provision that restricted recourse in certain situations.[43]

The CNCTR itself has broad powers to control the regularity of the techniques employed.[44]

OBLIGATIONS ON TELECOM OPERATORS AND HOSTING PROVIDERS

Legal or natural persons who provide cryptology services are to provide, within 72 hours of the request by authorized agents, encryption keys to allow decryption of data they encrypted. Authorized agents

[38] Decision n°2015-713 of 23 July 2015 (available at http://www.conseil-constitutionnel.fr/conseil-constitutionnel/root/bank/pdf/conseil-constitutionnel-144138.pdf)
[39] Id
[40] Article L. 822-2 of the French Internal Security Code
[41] Article L. 822-3 of the French Internal Security Code
[42] Article L. 841-1 of the French Internal Security Code
[43] Decision n°2015-713 of 23 July 2015 – *Considérant 49* (available at http://www.conseil-constitutionnel.fr/conseil-constitutionnel/root/bank/pdf/conseil-constitutionnel-144138.pdf)
[44] Articles L. 833-1 to L. 833-11 of the French Internal Security Code

may require the cryptology service provider to decrypt the data, unless the latter can demonstrate that it is not able to do it.[45]

Increasingly, smartphones operating systems allow for data encryption of the device (default setting for IOS) and manufacturers no longer possess the encryption key. In August 2015, Cyrus R. Vance Jr. (Manhattan district attorney), François Molins (Paris chief prosecutor), Adrian Leppard (Commissioner of the City of London Police), and Javier Zaragoza (Chief prosecutor of the High Court of Spain) co-authored a piece in the New York Times in which they denounced how phone encryption obstructs justice. The piece notes that "Apple and Google, whose operating systems are used in 96 percent of smartphones worldwide, announced [in September 2014] that they had re-engineered their software with "full-disk" encryption, and could no longer unlock their own products as a result."[46] François Molins warned in an interview in September 2015 that either Apple or Google should provide ways to decrypt data [encryption backdoors] when required by law enforcement or policy makers will have to pass law to constrain them to do so[47].

REMARKS

The French Data Protection Authority (*Commission Nationale de l'Informatique et des Libertés*, "CNIL") issued an opinion regarding the bill in March 2015. The document notes that the law allows for surveillance measures way broader and more intrusive than what was authorized so far by the previous legal framework.[48] Even though it acknowledges that privacy rights violations may be justified with respect to the legitimacy of the goal and the interests at stake, it reminds that such violations must be limited to what is strictly necessary, must be adequate and proportionate to the purposes, and appropriate safeguards and controls must be in place.[49] The CNIL welcomes the fact that under the new law, certain practices that were not subject to any type of control before are now subject to administrative and judicial control. However, the CNIL raised concern on several points of the law, notably the fact that an authorization implies automatic collection of log data. Such collection should only occur after a particular behavior has been flagged. The law disregarded this recommendation.

The law itself does not give any particular authority or power to the CNIL. Safeguards are ensured by the CNCT and ultimately the *Conseil d'Etat*. Even though intelligence gathering techniques are limited to certain purposes, the latter are so broad that it raises legitimate concern regarding people's privacy.

Recent Developments

In wake of the Paris attacks of 13 November 2015 that resulted in the death of 130 people and over 300 injured, the French President Francois Hollande declared the "state of emergency" in the speech he

[45] Article L. 871-1 of the French Internal Security Code
[46] http://www.nytimes.com/2015/08/12/opinion/apple-google-when-phone-encryption-blocks-justice.html?_r=1
[47] http://www.lexpress.fr/actualite/societe/francois-molins-les-nouveaux-telephones-rendent-la-justice-aveugle_1711458.html
[48] Opinion n°2015-078 of 5 March 2015 on intelligence bill (*Délibération n°2015-078 du 5 mars 2015 portant avis sur un projet de loi relative au renseignement*, available at http://www.cnil.fr/fileadmin/documents/approfondir/deliberations/D2015-078-PJLRenseignement.pdf)
[49] Id

gave the following day. The state of emergency officially started on 14 November 2015[50]. Created by law of 3 April 1955[51], the state of emergency allows for exceptional powers such as restrictions on people movement, temporary closing of theaters, allowing police home searches at any time (day and night), and measures to control the press and the media. It can only last for a period of twelve days unless extended by law. It was extended for a period of three months as from 26 November 2015 by law of 20 November 2015[52]. This law also created additional measures that can be allowed during a state of emergency (e.g. placing under house arrest any person against whom there are serious reasons to believe that his/her behavior constitutes a threat for security and public order)[53].

The Parliament also passed a law on 30 November 2015 relating to surveillance measures of international electronic communications[54]. Similar provisions from the surveillance law of 24 July 2015 had been invalidated by the Constitutional Council[55]. The new law reflects and took into account the arguments made by the Constitutional Council to invalidate the original provisions and introduces new provisions in the French Internal Security Code. According to this law, surveillance of communications issued or received abroad can be authorized only for the purposes of defense and promotion of the Nation's fundamental interests mentioned in article L. 811-3 (*see "scope of the law" section*)[56]. However, these provisions cannot be used for individual surveillance unless a special security measure has been issued against a person or the person has been identified as representing a threat to the Nation's fundamental interests.

The provisions set forth:

- The conditions under which the prime minister may authorize these international intelligence operations[57]
- Data retention requirements[58]

---

[50] Decree n°2015-1475 (available at http://www.legifrance.gouv.fr/eli/decret/2015/11/14/INTD1527633D/jo)
[51] Law n°55-385 of 3 April 1955 (available at http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000695350)
[52] Law n°2015-1501 of 20 November 2015 (available at http://www.legifrance.gouv.fr/affichTexte.do;jsessionid=8017112D004BA3A979F91514120BE4CF.tpdila07v_2?cidTexte=JORFTEXT000031500831&dateTexte=&oldAction=rechJO&categorieLien=id&idJO=JORFCONT000031500828)
[53] Id
[54] Law n2015-1556 of 30 November 2015 relating to surveillance measures of international electronic measures (available at http://www.legifrance.gouv.fr/affichTexte.do;jsessionid=998EACDA05B79BB46ECB1B480CC1846E.tpdila07v_2?cidTexte=JORFTEXT000031549747&dateTexte=&oldAction=rechJO&categorieLien=id&idJO=JORFCONT000031549744)
[55] Decision n°2015-713 of 23 July 2015 (available at http://www.conseil-constitutionnel.fr/conseil-constitutionnel/root/bank/pdf/conseil-constitutionnel-144138.pdf)
[56] Law n2015-1556 of 30 November 2015 relating to surveillance measures of international electronic measures (available at http://www.legifrance.gouv.fr/affichTexte.do;jsessionid=998EACDA05B79BB46ECB1B480CC1846E.tpdila07v_2?cidTexte=JORFTEXT000031549747&dateTexte=&oldAction=rechJO&categorieLien=id&idJO=JORFCONT000031549744)
[57] Article L. 854-2 of the French Internal Security Code

  - Communications are to be destroyed a year after their first use within the limit of four years as from the day they were collected
  - For log data: six years as from the day they were collected
  - For encrypted data: the delay starts as from the day they were decrypted within the limit of eight years as from the day they were collected
  - Extended retention periods are allowed in some circumstances: for technical analysis or if the data are part of a cyber-attack for example
  - In any event, data are to be destroyed as soon as they are no longer necessary for the purposes for which they were collected
- Powers of the CNCTR[59]
- Recourse for individuals[60]

The Constitutional Council, in a decision dated 26 November 2015, considered the law was conform to the Constitution, particularly the right to privacy, the right to secrecy of private correspondence, and the right to effective judicial recourse[61].

Overall, democracies around the world are struggling to address the threats of terror and the civil liberty challenges of law enforcement and surveillance efforts. This paper sought to provide insights into how one leading democracy has structured its balance of the human right to security and to privacy at one point in time.

[58] Article L. 854-5 of the French Internal Security Code
[59] Article L. 854-9 of the French Internal Security Code
[60] Individual recourse set forth in article L. 841-1 of the French Internal Security Code applies to these provisions
[61] Decision n°2015-722 DC of 26 November 2015 (available at http://www.legifrance.gouv.fr/affichTexte.do;jsessionid=998EACDA05B79BB46ECB1B480CC1846E.tpdila07v_2?cidTexte=JORFTEXT000031549759&dateTexte=&oldAction=rechJO&categorieLien=id&idJO=JORFCONT000031549744)