The Right to Privacy in the French Republic

Stakeholder Report
Universal Periodic Review
29th Session - France

Submitted by Privacy International

June 2017

Introduction

1. This stakeholder report is a submission by Privacy International (PI). PI is a human rights organisation that works to advance and promote the right to privacy and fight surveillance around the world.

2. Privacy International wishes to bring concerns about the protection and promotion of the right to privacy for consideration in France's upcoming review at the 29th session of the Working Group on the Universal Periodic Review.

Follow up to the previous UPR

3. In France's previous review, no express mention was made of the right to privacy in the context of data protection and communications surveillance in the National Report submitted by Pakistan or the report of the Working Group.

4. However, concerns on the right to privacy in relations to privacy, communications surveillance and data protection were expressed by some stakeholders.[1]

Domestic laws related to privacy

5. There is no specific personal data protection or privacy guarantee in the 1958 Constitution. Private and family life is protected under Article 9 of the Civil Code ("everyone has the right to respect for his private life").[2] Any victim of a privacy violation can claim damages and request that the violation be stopped. The Criminal Code also provides sanctions for offences against privacy.[3]

6. France was one of the first countries in Europe - indeed, in the world - to adopt a data protection law, the Law on Informatics, Files and Freedoms, which came into force in 1978. Article 1 of that Law establishes that "Information technology should be at the service of every citizen. Its development shall take place in the context of international co-operation. It shall not violate human identity, human rights, privacy, or individual or public liberties".[4]

International obligations

7. Protection of Privacy also comes from International and European treaties that have been ratified by France, including:

   a. Convention for the Protection of Human Rights and Fundamental Freedoms, Article 8.
   b. International Covenant on Civil and Political Rights, Article 17.
   c. Charter of Fundamental Rights of the European Union, Article 7.
   d. Convention on the Rights of the Child, Article 16.
   e. Convention on the Rights of Persons with Disabilities, Article 22.

AREAS OF CONCERN

I. Communications surveillance

8. Interception of telecommunications by the French intelligence and security community is regulated under a law dating back to 1991 and commonly referred to as the "Wiretapping Law".[5] The act authorized wiretapping for both law enforcement and national security purposes. Law enforcement were required to obtain judicial authorization from a magistrate judge, prior to the wiretapping, and were called to prove that such a wiretapping would be necessary for the purposes of an ongoing investigation. On the other hand wiretapping for national security purposes did not require such judicial authorization, and could be approved by the prime minister. The only safeguard established in the law for national security surveillance was a reporting obligation to an independent three-member Commission (described at greater length below).[6]

9. The Internal Security Code of 2012 solidified the practice laid down in the Wiretapping Law and expanded upon it.[7] The Code establishes a broad range of purposes that would justify interception of personal communications including: "national security, safeguarding the essential elements [of] scientific and economic potential of France, or the prevention of terrorism, crime and organized crime..."[8] Similar to prior legislation, the Code further clarifies that no prior judicial authorization is required for the conduct of such interception, instead the Prime Minister or those to whom he delegates this power may authorize these sort of operations.

10. The Code further expanded on the powers of the French intelligence community. It established that operations for the physical implementation of interceptions on the premises of the targets of surveillance, with or without the assistance of the network operators and telecom service providers, may be authorized by the telecommunications minister, or by those to whom he delegated this responsibility. The Prime Minister may additionally set a quote, and distribute this quote amongst the various agencies and departments, for the number of simultaneous communication interceptions that might be allowed at any given moment. This quote is then "brought to the attention" of the National Commission for the Control of Security Interceptions (La Commission Nationale de Contrôle des Interceptions de Sécurité, CNCIS). The CNCIS is comprised of a chairperson appointed by the President of France for a period of six years and accompanied by two serving parliamentarians from the National Assembly and the Senate. The CNCIS may review every single authorization for communications interception made by the Prime minister or those he designated. The Commission may additionally review complaints submitted by persons with "direct and personal interest".[9]

11. In December 2013 the Parliament of France adopted the Military Planning Law.[10] The law introduced certain amendments to the Internal Security Code and expanded even further on the powers of the French intelligence and security community. In particular, it allowed for the access to greater volumes of personal information including the content and metadata of phone conversations, emails, internet activity, personal location data, and other electronic communication data, as held by telecommunications and internet companies. Moreover, the law allowed for directly tapping the "network loads" of those companies, and the transmission of information in "real time" by the companies to the relevant agencies.[11]

The 2015 French Surveillance Law and its Aftermath

12. The “Surveillance Law” was introduced to Parliament on 19 March 2015 by French Prime Minister Manuel Valls as a reaction to the Charlie Hebdo shooting. The bill was adopted by a vote of 348 in favour and 86 against (42 abstentions) at the national assembly, and 252 in favour and 67 against (26 abstentions) at the Senate. It was made into law on 24 July 2015.[12] In addition to reaffirming existing laws and practices, which were already substantively permissive, the new legislation extended even more powers to the French intelligence and security community. The primary elements of the new legislation are the following:

    1. The list of justifications for the conduct of surveillance activities has been expanded and now covers the defence and promotion of the fundamental interests of France including as they relate to: (1) the national independence, territorial integrity, and national defence of France; (2) France’s major interests in foreign policy, the implementation of the European and international commitments of France, and the prevention of all forms of foreign interference; (3) the economic, industrial, and scientific interests of France; (4) the prevention of terrorism; (5) the prevention of (a) attacks on the institutions of the Republic; (b) the reestablishment of armed groups and private militias dissolved under Article L212-1 of the Internal Security Code; or (c) acts of collective violence which aim at harming public order and peace; (6) the prevention of crime and organized crime; (7) the prevention of the proliferation of weapons of mass destruction.[13]

    2. The CNCIS has been enlarged and is composed of nine members: (a) two deputies and two senators designated respectively for the duration of their term by the National Assembly and Senate respectively, ensuring a “pluralistic representation of parliament”; (b) two members of the State Council appointed by the Vice President of the State Council; (c) two judges outside of the hierarchy of the Cour de Cassation, appointed jointly by the President and by the Attorney General of the Cour de Cassation, and (d) a person qualified for his knowledge in electronic communications, appointed on the proposal of President of the Regulatory Authority for Electronic Communications and Postal.[14]

    3. Interception measures within the national territory of France may be requested by either the Ministers of Defence, Interior, or Finance, or anyone whom they designate. The law empowers the Government to unilaterally increase the number of intelligence agencies that might fall under the privy of these Minister’s interception request powers. Such requests are then sent in writing to the Prime Minister who will approve them following consultation with CNCIS. If the CNCIS provides an unfavourable opinion to a particular technique, the Prime Minister may nonetheless authorise the operation indicating the grounds for why the opinion of the CNCIS was not followed. Furthermore, in cases of “absolute emergency” the Prime Minister may authorize specific surveillance measures without prior notice to the CNCIS. This latter exception does not apply to the surveillance of parliamentarians, judges, lawyers, or journalists, surveillance of whom must involve a plenary session of the CNCIS.[15]

    4. Information collected must be destroyed after a period of 30 days and metadata collected may be stored for a period of five years. The law clarifies that as for encrypted communications, the period runs from the moment of their decryption (though in any event cannot be kept for more than six years after their collection).[16]

Furthermore, information containing “elements of a cyber-attack” may be stored for longer periods.

5. For the purpose of the prevention of terrorism, and for that purpose alone, the Government is granted new intrusive surveillance powers, including:

    - The installation of “automated” surveillance devices (also known as “black boxes”) at internet service providers and telecommunications companies to analyse all internet activities against specific algorithms set by the Government.[17] Additional technical devices might be introduced to collect and store metadata (including the identification and location of terminal equipment used, and the user subscription number and additional communication information).[18] Such devices grant French authorities direct access to the operators networks. No transparency surrounds any of these devices, the algorithms, or the selectors the Government is using.

    - The hacking into devices and computers, in cases where no other means are available. Authorization to hack general computer systems in order to locate, record, maintain and transmit information from a specific computer on that system or network, will be granted for a maximum period of 30 days. Authorization to access the specific computer and gain access to all that is displayed on a screen, and to information saved, conserved, or transmitted by the device, shall be granted for a maximum period of two months. All such authorizations are subject to possible renewal.[19]

    - Furthermore, the metadata of persons “previously identified as posing a threat” could be collected continuously and in “real-time,” directly from the operators’ networks. Such authorizations are issued for a period of two months and subject to possible renewable.[20] Some have argued that this broad provision grants the intelligence agencies the power to deploy “proximity sensors” and IMSI catchers, in the field, in order to ascertain the location and identification of particular targets.[21]

    - Finally, where there are serious grounds for believing that one or more persons communicating with an authorized subject of surveillance are themselves likely to provide information under the purposes that motivated the original authorization, they too might subject to surveillance (what is coined in surveillance terminology as a “hop”). This increases significantly the number of false positives and collateral data collected.

13. The “Surveillance Law” was the focus of great criticism by human rights experts and NGOs (including a petition signed by over 100,000 people).[22] The Human Rights Committee in its Concluding Observations in 2015 has too expressed concerns about original drafts of the law.[23]

14. Despite this opposition the Constitutional Court of France on 23 July 2015 reaffirmed the law, rejecting only a section of the law pertaining to “international surveillance,” conditions of which were found ill-defined (namely because the original bill referenced the collection of information which originated from outside of French territory, an ambiguous reference in the

age of internet communications).[24] On 30 November 2015 the French Government adopted an "International Surveillance Law", which reaffirmed the section quashed by the Constitutional Council with minor changes.[25]

15. Since the adoption of the Surveillance Act it has been challenged by 13 different complaints issued before the European Court of Human Rights. On 26 April 2017 the Fifth Section of the European Court of Human Rights communicated these complaints to France.[26]

II. Data Retention

16. The Data Retention Regulation in France, put in place before the *Digital Rights Ireland* Case, is still in force today. Internet Service Providers are instructed to delay by one year the deletion of significant amounts of identifiable metadata. Under Article 20 loi n. 2013-1168 of 18 December 2013, the French Defence Ministry and Home Office are allowed to access such retained information for purposes as broad as "national security", "the prevention of terrorism", the "preservation of the essential elements of France's economic and scientific potential".[27]

17. On 6 May 2015 civil society challenged the entire French data retention scheme under décret n°2011-219 du 25 février 2011 and article R. 10-13 du code des postes et communications électroniques in the French Conseil d'Etat court. The case is still pending. At the legislative and governmental level, there are no signs of imminent reform. This runs in contradiction to the the December 2016 judgment of the Court of Justice of the European Union (*Tele2/Watson)* which found indiscriminate retention of communication data to be incompatible with the right to privacy and of protection of personal data.[28]

III. France and Intelligence Sharing

18. On 16 November 2015, and in the wake of the 13th November terrorist attacks in Paris, the French Minister of State for European Affairs, Harlem Desir, urged EU member states to step up their intelligence sharing arrangements.[29] On 25 May 2017, following the terrorist attacks in Manchester, the U.K., recently elected president Emmanuel Macron was reported as pressing European States to enhance even further intelligence cooperation and information sharing.[30]

19. According to revelations made by former NSA contractor Edward Snowden, France is considered a "third party Signals Intelligence Designator" as part of its membership within the "9-Eyes" alliance. This alliance includes the permanent Five Eyes members (U.S., U.K., Australia, New Zealand, and Canada) alongside Denmark, the Netherlands, and Norway.[31] At least one report found that the nine share significant metadata.[32] France is also a party to a number of other intelligence sharing arrangements including the NATO Advisory Committee on Special Intelligence (NACSI) and the European "Club de Berne".[33]

20. There is no regulation of intelligence sharing under primary legislation in France and very little is known about the extent, nature, and scope of these arrangements, due to insufficient transparency and oversight.

IV. France and the Surveillance Industry

21. Based on Privacy International's "Surveillance Industry Index"[34] there are 45 surveillance technologies exporting companies headquartered in France, making it the third biggest HQ country in the world (following only the United States with 121 companies, and the United Kingdom with 104 companies). The surveillance exportation industry in France is worth according to some estimates 57 Billion U.S. Dollars".[35]

22. According to the Wall Street Journal, Amesys' Eagle monitoring centre, HQ in France, sold deep-packet inspection and analysis probes to Libya, which were later "deployed against dissidents, human-rights campaigners, journalists or everyday enemies of the state".[36] A criminal case against Amesys for complicity in acts of torture by the Gaddafi regime is ongoing.[37] This follows another judicial investigation that is underway in France against Qosmos, and a few other companies, for their involvement in selling of surveillance technologies to Bashar el-Assad's regime in Syria. NGOs FIDH and LDH have complained against these companies' alleged complicity in torture and other human rights violations in Syria.[38]

Recommendations

23. Based on the above observations we call on the government of France:

    1. Ensure that all interception activities conducted by the State under the 2015 surveillance law, and in particular the reliance on GPS trackers and IMSI catchers, automated processing using algorithms, are in conformity with international human rights protections of the right to privacy. All such surveillance measures must comply with the principles of legality, necessity, and proportionality, and subjected to adequate safeguards, notification requirements, and possibility for redress.
    2. Cease any acts of surveillance conducted by means of hacking to electronic devices through intrusive software, and launch a thorough assessment based on international human rights law (IHRL) to establish if hacking-based surveillance powers are compatible with the right to privacy.
    3. Refrain from imposing on telecommunication companies and third parties indiscriminate obligations to retain communications data, and should review its laws to ensure that any such obligations or requests to access such data are subject to tests of necessity and proportionality and authorized by judicial body, as required under European jurisprudence as reflected in the Watson/Tele2 decision of the CJEU.
    4. Review the practice of intelligence sharing with foreign agencies to ensure its compliance with the right to privacy, under IHRL. In particular, the Government should aim to ensure greater transparency surrounding these intelligence sharing arrangements, subject such arrangements to primary legislation and parliamentary scrutiny, and establish independent oversight mechanisms to prevent abuses in the course of these arrangements.
    5. Strengthen the regulation of the export of surveillance technologies by private companies registered or licenced in France. The Government should prevent the export of surveillance technologies where there is a risk they will be used to undermine human

rights, and should ensure that information surrounding its exports is made available to Parliament and the general public to foster greater accountability.

---

[1] The Human Rights League (LDH) expressed concern at the introduction of more and more new types of societal controls and surveillance mechanisms over the past 10 years. It recalled that, "as of June 2012, according to the National Commission for Information Technology and Civil Liberties (CNIL), 935,000 cameras were in operation in France. The number of police files had been steadily on the rise as well. LDH noted that files were also kept on persons by the French educational system and social welfare agencies. In addition, files were kept on foreign nationals and on persons under the guardianship of the court". For further reading see Summary prepared by the Office of the High Commissioner for Human Rights in accordance with paragraph 5 of the annex to Human Rights Council resolution 16/21, U.N. Doc. A/HRC/WG.6/15/FRA/3, available at https://documents-dds-ny.un.org/doc/UNDOC/GEN/G12/180/19/PDF/G1218019.pdf?OpenElement.

[2] CODE CIVIL [C. CIV] [CIVIL CODE] Art. 9 (Fr.).

[3] CODE PÉNAL [C. PÉN.] [PENAL CODE] Art. 226. The relevant parts of the Article are: "226-1: A penalty of one year's imprisonment and a fine of €45,000 is incurred for any willful violation of the intimacy of the private life of other persons by resorting to any means of: (1) intercepting, recording or transmitting words uttered in confidential or private circumstances, without the consent of their speaker; (2) taking, recording or transmitting the picture of a person who is within a private place, without the consent of the person concerned. Where the offences referred to by the present article were performed in the sight and with the knowledge of the persons concerned without their objection, although they were in a position to do so, their consent is presumed;226-2: The same penalties apply to the keeping, bringing or causing to be brought to the knowledge of the public or of a third party, or the use in whatever manner, of any recording or document obtained through any of the actions set out under article 226-1...226-5: Attempts to commit the offences set out under the present section are similarly punishable.226-8: A sentence of one year's imprisonment and a fine of €15,000 apply to the publication by any means of any montage made that uses the words or the image of a person without the latter's consent, unless it is obvious that it is a montage, or this fact is expressly indicated."

[4] Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés [Law 78-17 of January 6, 1978 Relating to Data, Files, and Freedoms], JOURNAL OFFICIEL DE LA RÉPUBLIQUE FRANÇAISE [J.O.] [OFFICIAL GAZETTE OF FRANCE], Jan. 25, 1978, Chapter 1: Principles and Definitions, Article 1.

[5] Loi n° 91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des télécommunications [Law 91-646 of July 10, 1991 relating to Secrecy of Correspondence Emitted by way of Electronic Communications], JOURNAL OFFICIEL DE LA RÉPUBLIQUE FRANÇAISE [J.O.] [OFFICIAL GAZETTE OF FRANCE], Jul. 13, 1991, p. 9167.

[6] For further reading on the law and its legislative history *see* Edwrd A. Tomlinson, *The Saga of Wiretapping in France: What it Tells Us About the French Criminal Justice System*, 53(4) LA. L. REV. 1091 (1993).

[7] CODE DE LA SÉCURITÉ INTÉRIEURE [C. SÉC. INT.] [INTERNAL SECURITY CODE] (Fr.)

[8] *Id.*, Book II, Part III, Article L241-2.

[9] The law further establishes additional safeguards including: (1) Each interception is logged, including date and time of the interception; (2) Of all the communicates that transpire through an intercepted bearer, a transcript may only be taken of communications relating to the abovementioned list of objectives; (3) All communications collected must be destroyed after ten days, at the latest, from the date it was originally made; (4) The transcripts of interceptions must also be destroyed once their retention is no longer necessary to fulfill the abovementioned objectives; (5) Information collected cannot be used for any other purposes other than those above listed; (6) The Parliamentary Committee for Intelligence (Délégation Parlementaire au Renseignement, DPR) established in 2007 was responsible for oversight of intelligence services, including in the context of this law. The DPR is comprised of four members from the Senate and four members from the national assembly. These oversight mechanisms and procedural safeguards do not apply, under the law, to the collection of communications transmitted via a "radio link". That would entail no oversight or limitations on interception of satellite and GSM communications. Moreover, the CNCIS and the DPR have been highly criticized for being ineffective in providing oversight over the intelligence operations of the French agencies. *See, e.g.*, Guillaume Champeau, La DGSI investie du pouvoir de surveiller les communications sur Internet, NUMERMA (2 May 2014), *available at*www.numerama.com/magazine/29260-dgsi-surveiller-communications-electroniques-internet.html; *See also*, EUROPEAN COMMISSION FOR DEMOCRACY THROUGH LAW (VENICE COMMISSION), UPDATE OF THE 2007 REPORT ON THE DEMOCRATIC OVERSIGHT OF THE SECURITY SERVICES AND REPORT ON THE DEMOCRATIC OVERISHGT OF SIGNALS INTELLIGENCE AGENCIES, para. 115 (2015).

[10] Loi n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale [Law 2013-1168 of December 18, 2013 on the Military Planning for the Years 2014 to 2019 and Containing Various Provisions Regarding Defense and National Security], JOURNAL OFFICIEL DE LA RÉPUBLIQUE FRANÇAISE [J.O.] [OFFICIAL GAZETTE OF FRANCE], Dec. 19, 2013, p. 20570.

[11] *Id.*, Article 20.

[12] Loi n° 2015-912 du 24 juillet 2015 relative au renseignement [Law 2015-912 of July 24, 2015 relating to Intelligence], JOURNAL OFFICIEL DE LA RÉPUBLIQUE FRANÇAISE [J.O.] [OFFICIAL GAZETTE OF FRANCE], Jul. 26, 2015, p. 12735.

[13] *Id.*, Article L811-3.

[14] *Id.*, Art. L831-1. The mandate of all members of the CNCIS, with the exception of the two deputies and two senators, is six years, non-renewable. The Commission establishes its own rules of procedure. The plenary session, which includes all members of the Commission, meets at least once a month. The commission will produce a yearly report. While respecting the confidentiality of the materials it reviews, the Commission may consult the Regulatory Authority for Electronic Communications and Postal. Note that the CNCIS may not consult any other party (namely human rights NGOs or privacy experts). On the other hand the law does recognize whistleblowing procedures, whereby intelligence agents may bring claims for illegalities before the CNCIS. The law further clarifies that in case of such whistleblowing, the whistleblower may not be subjected to punishment, or discrimination (either direct or indirect). For more on this process see Art. L861-3.

[15] *Id.*, Arts. L821-1-L821-7. For more on the powers of the CNCIS see Article L833.
[16] *Id.*, Art. L-822-2. Note that the law distinguishes information intercepted from regulation communication operations, and information intercepted through special operations involving the instalment of recording devices and cameras in private vehicles or premises. Such information may be collected for a period of up to 120 days.
[17] *Id.*, Art. L851-3. Based on the algorithmic analysis, if a person is identified as associated with "a threat of a terrorist nature" the Prime Minister or anyone delegated by him may authorize after consulting the CNCIS the collection of information on the person and other related data. The data is used within sixty days of this collection and are destroyed at the end of this period, except in case of "serious evidence confirming the existence of a terrorist threat attached to one or more of the persons concerned."
[18] *Id.*, Art. L851-6.
[19] *Id.*, Art. L-853-(1-2).
[20] *Id.*, Arts. L-851-2, L-851-5, L-856.
[21] IMSI catchers are mobile interception devices that are subject to US and European export controls, and have recently come under close scrutiny in US courts and legislatures. Because IMSI catchers are not targeted devices but identify and geolocate individuals within a given locale (such as a plaza or an airport) this would inevitably facilitate the surveillance of individuals who are not suspected of any crime.
[22] *See, e.g.*, *France: New Surveillance Law a Major Blow to Human Rights*, Amnesty International (24 July 2015), *available at* www.amnesty.org/en/latest/news/2015/07/france-new-surveillance-law-a-major-blow-to-human-rights/.
[23] Human Rights Committee, Concluding Observations on the Fifth Periodic Report of France, U.N. Doc. CCPR/C/FRA/CO/5, para. 12 (17 August 2015): "The Committee is concerned about the powers granted to the intelligence services for digital surveillance both within and outside France. The Committee is particularly concerned about the fact that the law on intelligence adopted on 24 June 2015 (submitted to the Constitutional Court) gives the intelligence agencies excessively broad, highly intrusive surveillance powers on the basis of broad and insufficiently defined objectives, without the prior authorization of a judge and without an adequate and independent oversight mechanism (art. 17). The State party should take all necessary steps to guarantee that its surveillance activities within and outside its territory are in conformity with its obligations under the Covenant, in particular article 17. Specifically, measures should be taken to guarantee that any interference in persons' private lives should be in conformity with the principles of legality, proportionality and necessity. The State party should ensure that the collection and use of data on communications take place on the basis of specific and legitimate objectives and that the exact circumstances in which such interference may be authorized and the categories of persons likely to be placed under surveillance are set out in detail. It should also ensure the effectiveness and independence of a monitoring system for surveillance activities, in particular by making provision for the judiciary to take part in the authorization and monitoring of surveillance measures."
[24] Conseil Constitutionnel [CC] [Constitutional Court], Jul. 23, 2015, n° 2015-713.
[25] The "International Surveillance Law" has three distinct features: 1. The law only applies to the monitoring of communications that are "sent or received abroad," which entails that their "communications subscription numbers or identifiers" are not traceable to the national territory of France. In case, it is later discovered, that information collected under the "international intelligence law" provisions involves wholly domestic communications, they must immediately bye subjected to the above discussed safeguards; 2. The Prime Minister may authorize the interception of all such foreign communications at the request of the relevant ministers, for the same justifications above listed and subject to the same renewal procedures above-discussed. Nonetheless, whereas domestic communications can be stored for up to 30 days, and metadata for up to 5 years, foreign communications can be stored for up to 12 months, and metadata for up to 6 years. Similar to domestic communications, the timing begins from the moment of decryption for encrypted information. However, encrypted information can be stored for up to eight years (and not six) and is cases of "strict necessity" may be stored for longer periods, similar to communications relating to elements of a cyber-attack; 3. The CNCIS should be informed of all decisions and authorizations under the act, and may issue investigations at its own initiative or following the complaint of any individual. Nonetheless, there is no requirement to consult the CNCIS prior to any such authorizations. See Loi n° 2015-1556 du 30 novembre 2015 relative aux mesures de surveillance des communications électroniques internationales [Law 2015-1556 of November 20, 2015 relating to Surveillance Measures of International Electronic Communications], JOURNAL OFFICIEL DE LA RÉPUBLIQUE FRANÇAISE [J.O.] [OFFICIAL GAZETTE OF FRANCE], Dec. 1, 2015, p. 22185.
[26] Association Confraternelle des Journalistes de la Presse Judiciaire and others v. France (49526/15); Martin v. France (49616/15); Lecomte v. France (49615/15); Babonneau v. France (49617/15); Souchard v. France (59618/15); Triomphe v. France (49619/15); Egre v. France (49620/15); Deniau v. France (49621/15); Ordre Des Avocats Au Barreau de Paris v. France (55058/15); Sur v. France (55061/15); Eydoux v. France (59602/15); Conseil National des Barreaux v. France (59621/15); Syndicat National des Journalistes and Federation Internationale des Journalistes v. France (5763/16).
[27] *See generally* Décret n°2011-219 du 25 février 2011 and article R. 10-13 du code des postes et communications électroniques (CPCE) (https://exegetes.eu.org/recours/abrogationretention/demande/2015-04-27-demande.pdf) and Article 20 loi n. 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 (L.246-1 to L.246-5 code de la sécurité intérieure) (law on military planning) (https://www.legifrance.gouv.fr/eli/loi/2013/12/18/DEFX1317084L/jo#JORFARTI000028338886. This information was compiled thanks to direct input from Lori Roussey, the Exégètes Amateurs (May 31st, 2017).
[28] Tele2 Sverige AB v. Post- Och telestyrelsen (C-203/15); Secretary of State for the Home Department v. Tom Watson et. al. (C-698/16), Joined Cases, Court of Justice of the European Union, Grand Chamber, Judgment (21 December 2016).
[29] Lawrence Norman & Valentina Pop, *EU Must Boost Intelligence Sharing, Says French Official*, THE WALL STREET JOURNAL (16 November 2015), *available at* www.wsj.com/articles/eu-must-boost-intelligence-sharing-says-french-official-1447669901.
[30] Marine Pennetier, *France's Macron calls for more European security cooperation and intelligence-sharing after Manchester attacks*, BUSINESS INSIDER (25 May 2017), *available at* http://uk.businessinsider.com/r-frances-macron-calls-for-stronger-european-security-cooperation-after-attacks-2017-5.
[31] Leo Kelion, *NSA-GCHQ Snowden Leaks: A Glossary of the Key Terms*, BBC NEWS (28 January 2014), *available at* www.bbc.co.uk/news/technology-25085592.
[32] Henrik Moltke & Sebastian Gjerding, *Denmark Part of the NSA Inner Circle*, INFORMATION (4 November 2013), *available at* www.information.dk/udland/2013/11/denmark-part-of-nsa-inner-circle.

[33] *See generally, Five Eyes, 9-Eyes, and many more*, ELECTROSPACES.NET (22 January 2014), *available at* http://electrospaces.blogspot.co.uk/2013/11/five-eyes-9-eyes-and-many-more.html.

[34] In August, 2016, Privacy International launched the "Surveillance Industry Index", the world's largest publicly available educational resource of data and documents of its kind on the surveillance industry, and an accompanying report charting the growth of the industry and its current reach. The SII, which is completely searchable, features over 1500 brochures and data on over 520 surveillance companies, as well as over 600 reported individual exports of specific surveillance technologies taken from open source records, including investigative and technical reports, as well as government export licensing data. For further reading *see* Edin Omanovic, *Privacy International launches the Surveillance Industry Index & New Accompanying Report*, PRIVACY INTERNATIONAL (1 August 2016), *available at* www.privacyinternational.org/node/912.

[35] For further reading *see* The Global Surveillance Industry, PRIVACY INTERNATIONAL (July 2016), *available at* https://privacyinternational.org/sites/default/files/global_surveillance_f.pdf.

[36] Margaret Coker and Paul Sonne, *Life Under the Gaze of Gadhafi's Spies*, The Wall Street Journal (14 December 2011), *available at* www.wsj.com/news/articles/SB10001424052970203764804577056230832805896.

[37] Business and Human Rights Resource Centre, Amesys Lawsuit (re Libya) (11 February 2015), *available at* https://business-humanrights.org/en/amesys-lawsuit-re-libya-0#c18496.

[38] For further reading *see* FIDH, France: Opening of a judicial investigation targeting Qosmos for complicity in acts of torture in Syria, Press Release (11 April 2014), *available at* www.fidh.org/en/region/europe-central-asia/france/15116-france-opening-of-a-judicial-investigation-targeting-qosmos-for-complicity.