PRIVACY INTERNATIONAL

Human Rights Committee, Privacy International
Submission: 114th Session, June-July 2015

The Right to Privacy in France

Submitted by Privacy International

Privacy International's submission in advance of the consideration of the periodic report of France, Human Rights Committee, 114th Session, 29 June – 24 July 2015

1 June 2015

Privacy International is concerned that electronic surveillance by French intelligence agencies and other bodies is overly broad, does not require prior judicial authorisation and it is not subject to effective oversight.

As such, Privacy International is concerned that the current law in France does not adequately protect from unlawful interference with the right to privacy, in violation of Article 17 of the International Covenant on Civil and Political Rights.

Regrettably, a new Intelligence bill recently adopted by the National Assembly and currently under consideration by the Senate grants new, highly intrusive powers to the intelligence agencies while failing to strengthen oversight.

Current law on interception of communications and oversight of intelligence services

Interception of telecommunications is regulated by the Internal Security Code (Code de la sécurité intérieure). Under the Code relevant intelligence and other agencies (from the Ministries of defence, interior and customs agencies) are given power to intercept personal communication for a broad range of purposes, such as "national independence, territorial sovereignty and national security", the protection of France's "scientific and economical potential," and the prevention of "terrorism", crime and organised crime (see Article L241-2 of the Internal Security Code.[1]). No prior judicial authorisation is required. Instead, authorisation is provided, upon written motivated request by the ministry in charge of the relevant intelligence services) by the Prime Minister (or delegated persons.)

These broad powers were further widened when, in December 2013, France adopted

1 Available here: http://www.legifrance.gouv.fr/affichCode.do;jsessionid=1857B46A14522506630D1138CFCFD600.tpdila13v_1?idSectionTA=LEGISCTA000025508253&cidTexte=LEGITEXT000025503132&dateTexte=20120618

Law No. 2013-1168 on Military Planning. Article 20 of the law introduces amendments to the Internal Security Code (Code de la sécurité intérieure).[2] The provision allows access to personal communications and metadata, including content of phone conversations, emails, internet activity, personal location data, and other electronic communication data, held by telecommunications and internet companies.

Oversight of interception of communications under the Internal Security Code is provided by the National Commission for the Control of Security Interceptions (CNCIS), composed of a chairperson appointed by the President and two serving parliamentarians (from the National Assembly and the Senate.) It reports to the Prime Minister and publish reports of its activities annually. Concerns have been expressed about the capacity of this body to effectively provide oversight, given its limited powers and its close link to the executive.[3]

More broadly, oversight of intelligence services is conducted by a Parliamentary body, established in 2007, composed of four members from the Senate and four members from the National Assembly. The Venice Commission noted how the "mandate and powers of the DPR have been criticised as inadequate and its membership as unconducive to serious oversight (the chairs of the Senate and Assembly Law and Defence committees sit ex officio)".[4]

The 2015 Intelligence Bill

On 5 May 2015 the National Assembly adopted by large majority a bill reforming intelligence surveillance in France.[5] The Bill was introduced by the government, following the attacks on Charlie Hebdo in January 2015, as an attempt to legalise already existing practices among intelligence agencies and to broaden surveillance powers under the guise of preventing terrorism.

Significant concerns about the Bill continue to be expressed by French and international non-governmental organisations.[6] Concerns focus in particular on the new, intrusive surveillance powers; the wide range of persons who could potentially be under-surveillance; and the significant powers entrusted to the Prime Minister, with no judicial prior authorisation and/or oversight of surveillance. These concerns are addressed in

---

2 Available here: http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000028338825&categorieLien=id

3 See for example, http://www.numerama.com/magazine/29260-la-dgsi-investie-du-pouvoir-de-surveiller-les-communications-sur-internet.html

4 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 oversight of signals intelligence agencies, 7 April 2015, available here: http://www.statewatch.org/news/2015/apr/coe-venice-commission-oversight-intelligence%20agencies-sigint-update-2015.pdf

5 See http://www.senat.fr/leg/pjl14-424.html

6 See https://sous-surveillance.fr/#/

more details in the following paragraphs.

The Bill grants government agencies a number of very intrusive surveillance powers.

Most notably, the Bill proposes to install surveillance technology at internet service providers and telecommunications companies to analyse all internet activity against specific algorithms set by the government. Such measures would introduce mass surveillance of personal communications, in a manner that is inherently disproportionate and indiscriminate, thereby violating Article 17 of the ICCPR. The fact that the information so collected remains unanalysed by intelligence agents until the Prime Minister requires the identification of the persons concerned does not allay the concerns that it amounts to an unlawful interference with the right to privacy. As the European Court of Human Rights has held, interception and/or storage of communications constitutes interference with the right to privacy irrespective of the subsequent use/analysis of the information collected.[7]

Further, the Bill permits intelligence agents to hack into devices and computers, as a technique of last resort. Hacking is an extremely intrusive form of surveillance and its use by any State authorities, particularly intelligence agencies, must be highly regulated to protect against abuses of power. Yet the Bill makes no provision for judicial authorisation or oversight of hacking powers.

The Bill also empowers the intelligence agencies to use "proximity sensors" in field surveillance in order to ascertain the location and identification of particular people. This provision is an attempt empower French intelligence agencies to use IMSI catchers, according to the Commission Nationale de l'Informatique et des Libertes, the French data protection authority, which was able to push the government to include a number of additional protections in the Bill prior to its publication. 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. The Bill stipulates that IMSI catchers can be used for collecting the live geolocation information of individuals using their devices. IMSI catchers are not devices targeting specific persons, instead they identify and geolocate individuals within a given area (such as a plaza or an airport.) As such, their deployment would inevitably facilitate the surveillance of individuals who are not the intended target of surveillance.

The Bill broadens significantly the potential target of communication surveillance, allowing the interception of electronic communications of anyone who may play an intermediary role, whether voluntary or not. As such intelligence agents would be authorised to intercept communications of those incidentally connected with a person of suspicion.

Retention of metadata collected as a result of the surveillance measures taken is

7 See Amman v. Switzerland (2000), Application 27798/95, paragraph 69.

permitted for five years. The term for the retention of encryption data only begins from the time the data is decrypted. Given the increase in encrypted communications, this provision, if adopted, would potentially mean that encrypted communications can be stored by intelligence agencies indefinitely. The risk of abuse, and the chilling effect of such measure on society are of particular concern.

Under specific provisions on "international surveillance", the surveillance powers of external communications granted by the Bill are vast and echo those currently being contested in the UK and the USA. They empower the French Prime Minister to order the interception of communications that are emitted or received from outside France ("les communications «émises ou reçues à l'étranger"). Given the structure of modern communications systems, this could apply to the digital communications of a vast, unspecified number of people, including those resident in France, whose communications are routed via server in a foreign country. The technical measures that intelligence agencies can implement to intercept such communications would be decided by the State Council in an unpublished decree, providing no opportunity for public scrutiny.

The Bill places unprecedented power in the hands of the Prime Minister's office, empowering it to authorise all forms of surveillance without having to seek the authorization of a court. While the law provides for the establishment of an expanded National Commission for the Control of Intelligence Techniques (according to the Bill, the Commission will have 13 members, of which 6 are members of parliament), the Commission's recommendations would not be binding on the Prime Minister and his or her delegates.

The lack of judicial authorisation and oversight of surveillance, particularly in light of the wide ranging surveillance powers envisaged in the Bill, is of particular concern. Judges are best suited to apply the legal tests to ensure that any interference with the right to privacy by intelligence or security agencies comply with the principles of necessity and proportionality. There is growing recognition by international experts and by national laws that it should only be carried out on the basis of a judicial order.[8] The same independent judicial authority should also ensure that any surveillance carried out is in compliance with such order and, more broadly, respect and protect the right to privacy.

Recommendations

Based on these observations, Privacy International suggests that the following recommendations are addressed to the French government:

- Take all necessary measures to ensure that its surveillance activities, both within

8 UN High Commissioner for Human Rights' report on the right to privacy in the digital age, UN doc. A/HRC/27/37, 30 June 2014. See also Human Rights Committee, Concluding Observations on the 4th U.S. report, 27 March 2014, para. 22, and European Court of Human Rights, *Kopp v. Switzerland* [1999] 27 EHRR 91, para. 74.

and outside France, conform to its obligations under the Covenant, including article 17; in particular, measures should be taken to ensure that any interference with the right to privacy complies with the principles of legality, proportionality and necessity, regardless of the nationality or location of the individuals whose communications are under surveillance;

- Amend current Intelligence Law Bill to ensure that it does not allow mass surveillance of communications and strictly regulate targeted surveillance, including by ensuring that collection of, access to and use of communications data are only allowed to the extent that they are necessary and proportionate to the pursuance of a legitimate aim; and by specifying in detail the precise circumstances in which any interception of communications may be permitted, the procedures for authorization, the categories of persons who may be placed under surveillance, the limit on the duration of such surveillance; and the procedures for the use and storage of data collected;
- Reform the current oversight system of surveillance activities to ensure its effectiveness, including by providing for judicial authorization and monitoring of surveillance measures, and establish an effective and independent oversight body with a view to preventing abuses.