Access Now submission to the Universal Periodic Review

France, Third Cycle

"Expanding surveillance state threatens privacy & free expression"

About Access Now

1. Access Now (www.accessnow.org) is an international organisation that works to defend and extend digital rights of users globally. Through representation in 10 countries around the world, including engagement with stakeholders and policymakers in France, Access Now provides thought leadership and policy recommendations to the public and private sectors to ensure the internet's continued openness and the protection of fundamental rights. We engage with an action focused global community, and our Technology Arm operates a 24/7 digital security helpline that provides real time direct technical assistance to users around the world.
2. Access Now advocates an approach to digital security that promotes transparent and accountable policies that protect human rights, including privacy and freedom of expression. Access Now has worked extensively in France, including on the increase in government surveillance, the court ruling on free expression and web blocking, protection of Net Neutrality, and government shutdowns of communications networks.
3. This is the third Universal Periodic Review for France, which was last reviewed in January 2013.

Domestic and international human rights obligations

4. France has ratified various international human rights instruments, including the International Covenant on Civil and Political Rights (ICCPR), the Convention against Torture (CAT), the International Covenant on Economic, Social and Cultural Rights (ICESCR), and the Convention on the Elimination of all Forms of Discrimination Against Women (CEDAW).
5. The Constitution of France provides for judicially enforceable fundamental rights such as freedom of expression. In 2009, the French Constitutional Court held that access to the internet is a crucial part of freedom of expression, and therefore a fundamental right.
6. France has historically been a country with a strong tradition of defending human rights. Despite this proud record, excessive counter terrorism and surveillance laws have resulted in abuses and violations of international human rights law in France.

Counter terror and surveillance laws

7. France has some of the most "expansive"[1] counter terrorism and surveillance laws in Europe, having passed no fewer than four separate laws extending its surveillance powers since December 2014. Together, these laws have made France an all-seeing state, capable of monitoring the population, collecting and retaining personal data for

[1] Human Rights Watch, "France: Don't Normalize Emergency Powers" (27 June 2017), available at https://www.hrw.org/news/2017/06/27/france-dont-normalize-emergency-powers.

excessive periods, and surveilling the private communications of individuals in France or abroad.

8. In March 2014, French newspaper *Le Monde* revealed a previously undisclosed relationship between French telco Orange and the French intelligence services, the Direction Générale de la Sécurité Extérieure (DGSE).[2] According to an internal document from Britain's Government Communications Headquarters (GCHQ) leaked by Edward Snowden, DGSE has an almost unlimited ability to spy on French citizens and international users by accessing a major, unnamed French telco's networks. The *Le Monde* article reports the telco in question as the French global telco giant Orange. The document details DGSE's close cooperation with the unnamed telco: together, they have worked to improve the French intelligence services' capabilities for interception on communication networks; develop encryption technologies; and break the encryption of data flowing through the network. According to the leaked document and *Le Monde*'s investigation, the DGSE has "free and total" access to Orange's networks and data passing through "without any oversight," and has shared this data with allied foreign intelligence services such as the GCHQ. It is not clear whether this unfettered access is only for Orange's operations in France, or includes its 30 networks and partner networks in Europe, the Middle East, Africa, and the Caribbean. In addition to nearly total access, the document alleges that the telco in question cooperates with the French government in order to break unspecified encryption protocols for data flowing over its networks. From large companies to journalists, many institutions and users employ encryption to protect the confidentiality of all types of data, including emails, documents, and phone calls.
9. In July 2015, the French Parliament passed the Projet de loi relatif au renseignement (**Intelligence Act**), a law that increases France's surveillance capabilities, and expands the power of the Executive Branch at the expense of users' rights to privacy and freedom of expression. The Intelligence Act was introduced through an emergency procedure following the Charlie Hebdo killings in January 2015, removing the possibility of much needed democratic debate in France. Pursuant to the Intelligence Act, internet providers are required to install mandatory "black boxes" that collect and store all internet connection data. Using algorithms to detect and report suspicious online behaviour, "black boxes" create an inherently disproportionate system of mass surveillance. Through the automated processing of data, black boxes are also likely to produce "false positives", placing innocent citizens under surveillance. The Intelligence Act also enables French intelligence agencies to intercept phone calls or access private communications, such as email without a court issued warrant. The Intelligence Act has been criticized by a large number of civil rights groups, technology companies, human rights defenders, lawyers, law enforcement organisations, and politicians over the clear violation of the right to privacy and the lack of judicial oversight of surveillance by French intelligence agencies. The UN Human Rights Committee also criticized the Intelligence

[2] Jacques Follorou, Espionnage: comment Orange et services secrets cooperent" (20 March 2014), available at http://www.lemonde.fr/international/article/2014/03/20/dgse-orange-des-liaisons-incestueuses_4386264_3210.html.

Act[3], raising concerns over the risks posed to human rights by "the extremely vast and invasive powers that the legislation gives to surveillance agencies" and the lack of appropriate judicial oversight and remedy mechanisms.[4] Despite these criticisms, in July 2015, the French Constitutional Court upheld the vast majority of the provisions within the Intelligence Act. While the Court declared that surveillance by French intelligence agencies in foreign countries is unconstitutional, the Court disregarded the serious concerns raised concerning the law's violation of the right to privacy.

10. In October 2015, France adopted the *Projet de loi sur la surveillance des communications internationales* (**Surveillance Act**). The Surveillance Act enables the indiscriminate mass surveillance of millions of individuals in France and abroad, with no mechanism for independent oversight or judicial control. The Surveillance Act:
    a. authorises the monitoring of communications that are sent or received abroad;
    b. enables the Prime Minister or one of his delegates to issue a permit to access personal data in order to obtain, among others, the geographic locations of organisations, groups, or individuals;
    c. provides for data retention periods of four, six, or eight years, depending on whether the information collected is content, metadata, or encrypted content that has been decrypted by the government, respectively; and
    d. allows for the indefinite retention of any information that is in any way pertaining to a "cyber attack," whether it is encrypted or not.

    At the same time as passing the Surveillance Act, France made several amendments to the Intelligence Act that created more extensive surveillance powers for French authorities. The amendments include requirements for:

    a. telecommunications companies to install "black boxes" on their networks, which use an algorithm to indiscriminately sweep data for suspicious activity;
    b. data to be retained from 30 days to four years, depending on the retention mandate and data type;
    c. collection of information and documents of individuals broadly identified as a threat;
    d. collection of login information (the access to which has been extended under the Surveillance law);
    e. creation of a commission, Commission Nationale de Contrôle des Techniques de Renseignement, to oversee the legality and justification for surveillance (which might nevertheless be overruled by the Prime Minister); and
    f. interception of any electronic communication likely to reveal intelligence information.
11. In November 2015, France declared a state of emergency in response to terrorist attacks in Paris which killed 132 people. While initially declared for only 12 days, the

[3] Privacy International "UN slams UK surveillance law, calls for privacy reforms in Canada, France and Macedonia (23 July 2015), available at https://www.privacyinternational.org/?q=node/629.
[4] Human Rights Committee, "Concluding observations on the fifth periodic report of France" (17 August 2015), available at http://tbinternet.ohchr.org/_layouts/treatybodyexternal/Download.aspx?symbolno=CCPR%2fC%2fFRA%2fCO%2f5&Lang=en.

state of emergency has been extended five times, and is currently set to sunset in July 2017.[5] In May 2017, President Macron issued a statement that he will request that the French National Assembly extend the state of emergency until 1 November 2017.[6] This drastic measure, barely used since World War II, has altered the normal balance of powers in France, and grants "authorities powers without judicial safeguards that undermine the rights to liberty, freedom of movement, privacy, security and freedoms of association and expression."[7] Pursuant to the state of emergency laws, French authorities are empowered to conduct warrantless searches of houses and electronic devices. Authorities were also authorised to access and copy data from electronic devices under re-authorisation of the state of emergency, before the French Constitutional court held this measure invalid. Human Rights Watch reports that French authorities have "carried out abusive and discriminatory raids and house arrests against Muslims" under the state of emergency law that have "created economic hardship, stigmatized those targeted, and have traumatized children."[8]

12. In that context, in November 2015, France informed the Council of Europe Secretary General of its intention to Derogate of certain rights, including the right to free expression and the right to privacy, protected under the European Convention on Human Rights, due to the state of emergency.[9] Such a derogation is authorised pursuant Article 15 of the Convention in times of public emergency threatening the life of a nation but raises serious concerns towards France's commitment to the respect and protection of these rights given the several extensions of the state of emergency.
13. In January 2016, David Kaye, Special Rapporteur on the freedom of opinion and expression; Maina Kiai, Special Rapporteur on the rights to freedom of peaceful assembly and of association; Michel Forst, Special Rapporteur on the situation of human rights defenders; Ben Emmerson, Special Rapporteur on the protection and promotion of human rights and fundamental freedoms while countering terrorism; and Joseph Cannataci, Special Rapporteur on the right to privacy, issued a joint statement condemning the state of emergency and surveillance laws in France on the basis that they impose "excessive and disproportionate restrictions on fundamental freedoms."[10] The independent UN experts expressed concern over "the lack of clarity and precision of

---

[5] Agence France-Press, "French parliament votes to extend state of emergency until after 2017 elections" (14 December 2016), available at https://www.theguardian.com/world/2016/dec/14/french-parliament-votes-to-extend-state-of-emergency-until-after-2017-elections.

[6] France 24, "France's Macron seeks to extend state of emergency to November" (24 May 2017), available at http://www.france24.com/en/20170524-france-president-macron-seeks-extend-state-emergency-manchester.

[7] Human Rights Watch, "France" (2017), available at https://www.hrw.org/europe/central-asia/france.

[8] Human Rights Watch, "France: abuses under state of emergency" (3 February 2016), available at https://www.hrw.org/news/2016/02/03/france-abuses-under-state-emergency

[9] France informs Secretary General of Article 15 Derogation of the European Convention on Human Rights (25 November 2015), available at http://www.coe.int/en/web/secretary-general/news/-/asset_publisher/EYlBJNjXtA5U/content/france-informs-secretary-general-of-article-15-derogation-of-the-european-convention-on-human-rights

[10] Office of the High Commissioner for Human Rights, "UN rights experts urge France to protect fundamental freedoms while countering terrorism" (19 January 2016), available at http://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=16966&LangID=E.

several provisions of the state of emergency and surveillance laws, related to the nature and scope of restrictions to the legitimate exercise of right to freedom of expression, freedom of peaceful assembly and association and the right to privacy."[11] The experts recommended reforming these laws to ensure they comply with international human rights law, in particular noting the importance of "the adoption of prior judicial controls over anti-terrorism measures."[12]

14. Despite these recommendations, in July 2016, following terrorist attacks in Nice, the National Assembly extended the state of emergency for six months and also passed new counter-terrorism laws. Under these laws, French authorities can undertake warrantless searches of luggage and cars, and carry out identity checks. During administrative searches, law enforcement can also collect and store personal data and files from electronic devices. Finally, law enforcement can wiretap and surveil not only suspected individuals but also a "close circle" of acquaintances.
15. In October 2016, French Constitutional Council declared unconstitutional a section of the Intelligence Act. The Intelligence Act authorised, without meaningful privacy safeguards or oversight, authorities to monitor and control wireless communications. In its decision, the council found that due to their disproportionate scope, unlimited purpose and a lack of safeguards and oversight mechanism, the measures violated "the right to privacy and the confidentiality of communications" and are therefore unconstitutional.[13] However, the Council did not entirely strike down the practice, and set out a December 2017 deadline for the government to adopt a new law that includes the necessary robust safeguards for human rights. The decision is an opportunity for the French government to bring the law in line with human rights obligations. We encourage lawmakers to apply the International Principles on the Application of Human Rights to Communications Surveillance[14] to the review of measures on the surveillance of wireless communications, and indeed, to every form of communications surveillance in France. Authorities should not be able to bypass human rights protections for communications because of how they take place, and there is no reason to implement a lower standard for mobile communications than for those that take place using a fixed line. To assist in that process, Access Now has developed an implementation guide for putting the principles into practice.[15]

---

[11] Office of the High Commissioner for Human Rights, "UN rights experts urge France to protect fundamental freedoms while countering terrorism" (19 January 2016), available at http://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=16966&LangID=E.
[12] Office of the High Commissioner for Human Rights, "UN rights experts urge France to protect fundamental freedoms while countering terrorism" (19 January 2016), available at http://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=16966&LangID=E.
[13] Conseil Constitutionnel, "Décision n° 2016-590 QPC du 21 octobre 2016 - La Quadrature du Net et autres [Surveillance et contrôle des transmissions empruntant la voie hertzienne]" (21 October 2016), available at http://www.conseil-constitutionnel.fr/conseil-constitutionnel/francais/les-decisions/acces-par-date/decisions-depuis-1959/2016/2016-590-qpc/communique-de-presse.148048.html.
[14] "Necessary and Proportionate: International Principles on the Application of Human Rights to Communications Surveillance" (May 2014), available at https://necessaryandproportionate.org/principles.
[15] Access Now, "Universal Implementation Guide for the International Principles on the Application of Human Rights to Communications Surveillance" (May 2015), available at https://necessaryandproportionate.org/files/2016/04/01/implementation_guide_international_principles_2015.pdf.

16. On 22 June 2017, the French government introduced a new counterterrorism bill, the Draft Law to Strengthen Internal Security and the Fight Against Terrorism.[16] The draft law gives enhanced powers to local representatives of the Minister of Interior, called "Prefects" and proposes "changes to surveillance legislation, border controls, and processes for retaining the data of passengers arriving by sea or airplane."[17] Under the draft law, Prefects are able "to designate public spaces as security zones, limiting who could enter and leave them; to limit the movement of people considered a national security threat; to close mosques and other places of worship; and to search private property."[18] The first three of these powers are not subject to judicial oversight. These powers violate the right to freedom of movement, assembly and association, as well as the right to private and family life.

Business & human rights in telecommunications

17. Positively, on 21 February 2017, France's Parliament adopted a bill imposing obligations on large French companies to undertake human rights due diligence regarding their operations, the operations of their subsidiaries, and their supply chains. Pursuant to the law, large French companies are required to "establish, publish and implement a vigilance plan" and "take appropriate measures to identify and prevent risks of infringements to human rights and fundamental freedoms."[19]
18. French telecoms companies have operations all around the world, in particular in the MENA region and Sub-Saharan Africa, where governments routinely request telecom companies to disrupt, block, throttle, and shut down access to networks, applications, and services. In particular, a significant number of intentional disruptions, timed to interfere with freedom of expression -- what we term "internet shutdowns" -- have been documented over the past two years. Given the fact that access to the internet must be considered as a fundamental right based on jurisprudence from the French Constitutional Court, French telecom companies should reflect this commitment and take every measure to ensure their operations respect freedom of expression online. To this end, their obligations under the new due diligence law could help identifying and preventing risks of shutdowns in countries where these companies have operations.

Recommendations

19. France can improve its human rights record and treatment of digital rights in several areas. We accordingly recommend that the government of France:

---

[16] Legifrance, "Projet de loi renforçant le sécurité intérieure et la lutte contre le terrorisme (INTX1716370L)" (22 June 2017), available at https://www.legifrance.gouv.fr/Droit-francais/Actualite/22-juin-2017-securite-interieure-et-lutte-contre-le-terrorisme.
[17] Human Rights Watch, "France: Don't normalize emergency powers" (27 June 2017), available at https://www.hrw.org/news/2017/06/27/france-dont-normalize-emergency-powers.
[18] Human Rights Watch, "France: Don't normalize emergency powers" (27 June 2017), available at https://www.hrw.org/news/2017/06/27/france-dont-normalize-emergency-powers.
[19] Office of the High Commission for Human Rights, "UN expert group welcomes legislative efforts in France and other countries to address adverse business human rights impacts" (23 March 2017), available at http://www.ohchr.org/Documents/Issues/TransCorporations/2017-03-23_INFONOTEFRANCESUPPLYLAW.pdf.

a. Restrict law enforcement, intelligence agency, and national security authority access to user data in the Intelligence Act and Surveillance Act;
b. Amend the provisions regarding surveillance and access to personal information in the Intelligence Act and Surveillance Act to ensure that law enforcement and intelligence only interfere with privacy to the extent necessary and proportionate in pursuit of a legitimate aim;
c. End the state of emergency;
d. Protect, rather than obstruct or interfere with, the use of encryption, an essential enabler of the rights to privacy and freedom of expression in the digital age;
e. Ban government hacking, with any exception conducted under strictly defined safeguards;
f. Commit to enhancing freedom of expression online and preventing violations by state and non-state actors, such as telecom companies, and holding them to strict standards of transparency and accountability, while also avoiding a shift of responsibility for enforcing human rights to private companies alone;
g. Develop a strategy for fast, reliable and secure connectivity in the whole French territory and continue strengthening internet connectivity throughout the French speaking world, and work with governments to prevent intentional shutdowns and disruptions; and
h. Promote investments into privacy and data protection friendly digital products and services.

20. The UPR is an important U.N. process aimed at addressing human rights issues all across the globe. It is a rare mechanism through which citizens around the world get to work with governments to improve human rights and hold them accountable to international law. Access Now is grateful to make this submission.
21. For additional information, please contact Access Now General Counsel Peter Micek (peter@accessnow.org).