Submission to report on the Right to Privacy in the Digital Age by the Office of the UN High Commissioner for Human Rights

April 2018

Introduction

Access Now welcomes the opportunity to submit comments and recommendations to the Office of the High Commissioner for Human Rights (OHCHR).[1] Since our inception, Access Now has engaged with the United Nations in support of our mission to extend and defend the digital rights of users at risk. By combining direct technical support, comprehensive policy engagement, global advocacy, grassroots grantmaking, and convenings such as RightsCon, we fight for human rights in the digital age. Since July 2016, Access Now has special consultative status at the UN Economic and Social Council.

Access Now **provided comments** to all issues listed in the consultation. These **comments support the following recommendations** that we present for consideration for the High Commissioner's report.

Recommendations

- ***Surveillance and communications interception***
    - Government mass surveillance should be banned for its unnecessary & disproportionate restriction of a range of human rights.
    - Legal and technical surveillance capabilities must not be abused to target vulnerable communities.
    - Government should seek a warrant prior to conducting targeted surveillance.
    - Surveillance tools, including software and equipment, should not be provided to governments which are likely to use them to undermine the rights of human rights defenders like activists and journalists.
    - Government hacking should be presumptively banned globally.
    - Exporting countries should disclose licenses, information about products, end users, destination countries and their human rights records, potential human rights impacts of the technology and other relevant information.
    - Governments should have a vulnerability disclosure process that prioritizes disclosure and mitigation when they find or become aware of technology flaws.
    - Governments should facilitate coordinated vulnerability disclosure (CVD) within their jurisdiction.

[1] *About Us*, Access Now, https://www.accessnow.org/.

- *Encryption and anonymity*
    - Governments should not seek to undermine encryption, for instance through backdoors or weakened standards.
    - Governments should discourage private platforms from imposing identity policies which put anonymity at risk
    - In designing and implementing their own digital identity systems, governments should prioritize user privacy by ensuring that such systems prioritize secure communications by encrypting traffic end-to-end during authentication and using other identity-related procedures.

- *National legislative and regulatory frameworks concerning the collection, processing, retention or use of personal data by Governments and other actors*
    - Government should develop binding frameworks to ensure the right to data protection, alongside the right to privacy.
    - Government should not mandate blanket data retention.
    - Government should prevent the use of invasive tracking and profiling.
    - Enforce data protection, privacy, and transparency obligations on security firms and data brokers, who often go underregulated.

- *Growing reliance on data-driven technology and biometric data*
    - Public and private sector entities should abide by the principles of security, data protection, and privacy by design, and strive for data minimization at all times.
    - Governments should not mandate the collection of biometric data in digital identity programmes.
    - Governments should not create centralised databases of individuals' biometric data.

- *Undue interferences with the right to privacy in the digital age that may have particular effects on vulnerable or marginalised groups, and based on a person's perceived gender, age, religion, sexual orientation, and other characteristics*
    - Governments and businesses should consider that vulnerable groups, marginalised populations, and minorities are often the first and most significantly impacted by ill-conceived policies.
    - Governments should implement and enforce legislation that promotes the right to information, right to object, and right to explanation linked to the use of algorithms and AI, as these technologies particularly impact marginalised groups.

- *Procedural and institutional safeguards*
    - The United Nations and states should protect the right to privacy, a universal and enforceable human right.
    - States should endorse and codify the International Principles on the Application of Human Rights to Communications Surveillance.

- Individuals should be afforded legal remedies for measures that impact their right to privacy, including unlawful or arbitrary state surveillance.

Comments on the list of issues

1) Recent developments in national or regional legislation, case law, and practice concerning the right to privacy in the digital age

The Universal Declaration of Human Rights (UDHR) recognises the right to privacy as a fundamental right and states that this right should not be subjected to arbitrary interference.[2] Currently, 160 countries refer to the right to privacy in their respective constitution, however the application of this right is ever changing due to the growing interest among corporate and state actors to promote significant data collection and retention.[3]

The recent Cambridge Analytica data breach exposes this issue. In 2014, a group of social scientists led by Aleksandr Kogan developed and deployed a personality test called "thisisyourdigitallife."[4] This application allowed researchers to access information of at least 87 million individuals, though only 270,000 users actually downloaded the app. Subsequently, Kogan's company contracted to disclose the collected data to Cambridge Analytica, company which used this data to develop targeted advertisements for the 2016 US presidential election.[5]

Incidents of this magnitude are not uncommon. Abusive data sharing practices and data breaches have been growing exponentially, hence states' willingness to enforce privacy and data protection rights against further harm by private actors - and rightfully so.[6]

However, governments seem less interested in curtailing state surveillance, and often justify their behaviour under the counterterrorism, cybersecurity and domestic crime banners. For instance in January 2018, the United States Congress re-authorised and expanded Section 702 of the FISA Amendments Act. This act allows

---

[2] *A Human Rights Response to Government Hacking,* Access Now, https://www.accessnow.org/cms/assets/uploads/2016/09/GovernmentHackingDoc.pdf.
[3] *Creating A Data Protection Framework: A Do's and Don't Guide for Lawmakers*, Access Now, https://www.accessnow.org/cms/assets/uploads/2018/01/Data-Protection-Guilde-for-Lawmakers-Access-Now.pdf.
[4] *It's Not a Bug, It's A Feature: How Cambridge Analytica Demonstrates the Desperate Need for Data Protection*, Access Now https://www.accessnow.org/its-not-a-bug-its-a-feature-how-cambridge-analytica-demonstrates-the-desperate-need-for-data-protection/.
[5] *Id.*
[6] *2017 Poor Internal Security Practices Take a Toll - Findings From The First Half of 2017 Breach Level Index*, Gemalto, http://breachlevelindex.com/assets/Breach-Level-Index-Report-H1-2017-Gemalto.pdf.

the government to conduct excessive, disproportionate and warrantless surveillance.[7] Most surveillance technologies, like those used by the US government, permit states to intercept private communication, including records of conversations, text messages, emails, search history and contact list, as well as allows for remote access to both the phone's camera and microphone.[8]

States also rely on surveillance software to silence dissenting voices. According to leaked documents from Hacking Team, a surveillance software company, the Egyptian, Italian, Korean, Turkish, Mexican, Indian, and Colombian governments purchased surveillance software from this company. In August 2017, civil society organization CitizenLab and Mexican partners documented at least 21 cases where the government used Pegasus, software developed by Israeli/American cyberarms dealer NSO Group, in order to target journalists, human rights lawyers, activists, and political figures. Accountability remains out of reach for victims of these targeted hacking tools, as governments do not disclose their export, import, authorization, or procurement, and courts have not held law enforcement to account for their use. There is also a global trend for states to revise or promulgate laws that authorise government hacking, including the codification of extraterritorial reach of domestic laws.[9]

2) *Surveillance and communications interception:*

a) Government surveillance, including, for example, communications interception and bulk data collection and processing, targeted intrusions in ICT systems and issues relating to cross-border surveillance and access to personal data.

i) Government surveillance

- For many years now, International human rights bodies, regional courts, and experts have found mass surveillance to be in violation of human rights law. In 2016, the UN High Commissioner for Human Rights indicated that "[m]ass secret surveillance is not permissible under international human rights law, as an individualised necessity and proportionality analysis would not be possible in the context of such measures."[10]
- Access Now has reported several instances of legislation establishing mass surveillance to the United Nation through the process of Universal Periodic Review:

---

[7] *Access Now Opposes Proposal to Extend Warrantless Surveillance*, Access Now, https://www.accessnow.org/access-now-urges-u-s-congress-vote-proposal-extend-warrantless-surveillance/.

[8] *Submission to the Joint Committee on the Draft Investigatory Powers Bil*l, Privacy International, 21 Dec. 2015, https://privacyinternational.org/sites/default/files/2017-12/Submission_IPB_Joint_Committee.pdf

[9] *Government Hacking is no Answer to the MLAT Problem*, Megan White, https://www.accessnow.org/government-hacking-no-answer-mlat-problem/.

[10] *A/HRC/33/29 - Report on Best Practices and Lessons Learned on How Protecting and Promoting Human Rights Contribute to Preventing and Countering Violent Extremism,* Security Council Counter-Terrorism Committee, https://www.un.org/sc/ctc/news/document/ahrc3329-report-on-best-practices-and-lessons-learned-on-how-protecting-and-promoting-human-rights-contribute-to-preventing-and-countering-violent-extremism/.

- In 2017, we reported on the publication of confidential documents in 2014 in Germany which revealed that the Bundesnachrichtendienst (BND) requested an additional 300 million Euros from the German Parliament to expand its surveillance programme. The programme is intended to overhaul the BND's digital infrastructure and enhance Germany's surveillance and metadata collection capability.[11] In June 2017, the German Parliament also passed a bill allowing the government to hack into encrypted messaging services during certain criminal investigations. The legislation permits the use of spyware to infiltrate a suspect's device and read messages before they are encrypted, allowing remote searches on a suspect's device in especially severe cases.[12]
- In 2016, Brazil hosted the Olympic and Paralympic Games. The preparation for them, the country's invested in mass surveillance technologies such as cameras, integrated command centers that can track conditions in real time and allow for coordinated responses by different municipal, state, and federal departments, surveillance balloons equipped with monitoring systems that were originally developed for military use and the country also monitored social media accounts of participants of protests. Despite the potential abuses to the right to privacy these mass surveillance technologies represent, they were not followed by a proper public debate on their future uses or transparency measures as to their acquisition and use. There are also serious regulatory gaps regarding the limits and rules in which they will be implemented.[13]
- In 2017, we indicated that France has some of the most "expansive"[14] counterterrorism 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 excessive periods, as well as surveilling the private communications of individuals in France or abroad.[15] Since then, France have further codified measures creating risks for the right to privacy by for instance integrating exceptional and repressive measures from the state of emergency into ordinary law.[16]
- In 2016, we reported on the negotiations of the UK Investigatory Power Bill, now Act, which creates significant risks for digital security, the right to privacy and the rules of law, but

[11] *Netzpolitik.org Reports on Government Surveillance, is Investigated for Treason*, Estelle Massé, https://www.accessnow.org/netzpolitikorg-reports-on-government-surveillance-is-investigated-for-trea/.
[12] *German Government to Spy on Encrypted Messaging Services*, Victor Brechenmacher, http://www.politico.eu/article/german-government-to-spy-on-encrypted-messaging-services/.
[13] *Access Now Submission to the United Nations Human Rights Council, on the Universal Periodic Review 2016 Cycle for Brazil,* Access Now, https://www.upr-info.org/sites/default/files/document/brazil/session_27_-_may_2017/accessnow_upr27_bra_e_main.pdf.
[14] *"France: Don't Normalize Emergency Powers"*, Human Rights Watch https://www.hrw.org/news/2017/06/27/france-dont-normalize-emergency-powers.
[15] *Acess Now at the United Nations: Spyware in the UAE, Surveillance in France and Shutdowns in Africa*, Peter Micke and Cole Potter, https://www.accessnow.org/access-now-united-nations-spyware-uae-surveillance-france-shutdowns-africa/.
[16] *France's Permanent State of Emergency,* Marco Perolini, https://www.amnesty.org/en/latest/news/2017/09/a-permanent-state-of-emergency-in-france/.

among other things, allosing for bulk interceptions, communications surveillance and equipment interferences.[17]

- Despite opposition from international bodies and important regional rulings, government continues to expand their surveillance. For instance, in the December 4, 2015 ruling on the case of Roman Zakharov v. Russia, the European Court of Human Rights declared the system of secret interception of mobile telephone communications a violation of Article 8 of the European Convention on Human Rights referring to the protection of private life.[18] However, in 2016, Russia adopted the Federal Security Service law which include provisions undermining the security and privacy of users.
- Subsequently, in Szabo and Vissy v. Hungary (ECtHR, Application no. 37138/14) the European Court of Human Rights declared that Hungarian surveillance law infringes the rights to privacy, and the Court reinforced its findings of Zakharov v. Russia. Szabo concerned the powers of the Hungarian intelligence agency, the Anti-Terrorism Task Force (TEK), under the Police Act of 1994. The Act provided one set of surveillance powers exercisable in the context of criminal investigations (which subjected surveillance to judicial authorization), and another set of powers applicable to intelligence gathering in the context of national security. The national security surveillance powers were subject to ministerial, rather than judicial, authorization; were not linked to a particular crime; and required a warrant to relate only to a premises, persons concerned, or "a range of persons," and was thus potentially executable against any person.[19] The judgment offers further interpretation of "reasonable suspicion", it has introduced a "strict necessity" standard[20], and added stricter language on judicial authorisation[21].
- Similarly, the US has one of the most invasive surveillance infrastructures in the world, both in terms of technological reach and legal authority. Despite the passage of the USA Freedom Act in 2015 which provided for some limitation to surveillance activities by ending bulk collection under certain authorities, like Section 215 of the FISA Amendments Act, the US has then reinitiated the surveillance race to the bottom.[22] In 2015, the Executive Order 12333 was expanded to allow the distribution of "raw" surveillance data collected by the National Security Agency with 16 other government agencies. Foreign intelligence collected under this executive order does not require any congressional or judicial authorisation and there is little transparency about how it is carried out.[23] Furthermore, in January

---

[17] *Access Now Submission to the United Nations Human Rights Council, on the Universal Periodic Review 2016 Cycle for the United Kingdom*, Access Now, https://www.accessnow.org/cms/assets/uploads/2016/09/UPR-UK-2016.pdf.

[18] *Case of Roman Zakharov v. Russia*, European Court of Human Rights Cours Europeenne Des Droit De L'Homme,http://www.statewatch.org/news/2015/dec/echr-russian-secret-surveillance-judgment.pdf. }.

[19], The European Court of Human Rights Constrains Mass Surveillance (Again), Carly Nyst, https://www.justsecurity.org/28939/ecthr-constrains-mass-surveillance/.

[20] Secret surveillance must be strictly necessary in two senses, the Court said: (1) It must be strictly necessary as a general consideration for the safeguarding of democratic institutions; and (2) it must be strictly necessary as a particular consideration for the obtaining of vital intelligence in an individual operation (para. 73).

[21] "in this field, control by an independent body, normally a judge with special expertise, should be the rule and substitute solutions the exception, warranting close scrutiny"

[22] *The USA FREEDOM Act of 2015: What's in it?,* Amie Stepanovich, https://www.accessnow.org/the-usa-freedom-act-of-2015-whats-in-it/.

[23] *Letter to Commissioner Vera Jourova*, Fanny Hidvégi and Amie Stepanovich, https://www.accessnow.org/cms/assets/uploads/2017/02/Letter-to-Jourova.pdf.

2018, the United States re-authorised and expanded Section 702 of the FISA Amendments Act which is used to authorise excessive, disproportionate and warrantless surveillance.[24] Finally, while technology has made it easier to obtain the communications of people in bulk, not only has the US government continued to refuse to recognise the human rights of users around the world, but the US intelligence community have even specifically refused to establish even a point of contact for human rights abuses.[25]

ii) Government hacking

- Government hacking interferes with human rights as embodied in international treaties and declarations including rights to privacy, free expression, and due process. Government hacking is often more invasive than other forms for government surveillance and therefore **government hacking should be presumptively prohibited.**[26]
- With robust protections, it may be possible, though still not necessarily advisable, for a government to overcome the presumptive prohibition against government hacking for surveillance or intelligence gathering. We have noted that the circumstances under which it could be overcome are both limited and exceptional, and in our dedicated report on the subject we identified ten strong safeguards, including vulnerability disclosure and oversight, that must both be implemented and complied with to meet that standard.[27] Absent government compliance with all ten safeguards, the presumptive prohibition on hacking remains.

b) **Role of business enterprises in contributing to, or facilitating government surveillance activities, including:**

i) Sale of surveillance technology by business enterprises and ensuing responsibilities;

- Export control rules should **stop surveillance equipment from being exported into countries where there is a high risk that it would be used to undermine the rights of civil society actors like activists, human rights defenders, and journalists**.[28]
- Exporting countries should **annually disclose information about importing countries,** including licenses approval, denials, the equipment in question, the product description, cost, as well as the end user.[29]
- **Surveillance exporting countries should also take a firm stand in order to defend the freedom to inform.** Traditionally journalists are among the groups most targeted by "dual-use" technologies which also have a chilling effect not only on them but also their sources, fuelling concern about the security of

[24] *Supra note 7*.
[25] *Intelligence Community Refuses to Follow Treaty Requirements on Human Rights*, Amie Stepanovich, https://www.accessnow.org/intelligence-community-refuses-follow-treaty-requirements-human-rights-2/.
[26] *Supra note 2*.
[27] *Id*.
[28] *EU: European Parliament Must Vote to Stop Surveillance Equipment Going to Rights-Abusing Governments*, Access Now, https://www.accessnow.org/eu-european-parliament-must-vote-stop-surveillance-equipment-going-rights-abusing-governments/.
[29] *Shared Statement on the Update of the EU Dual-Use Regulation*, Access Now, May 2017, https://www.accessnow.org/cms/assets/uploads/2017/05/NGO_Sharedstatement_dualuse_May2017.pdf.

their communications and therefore discouraging an exchange of information. Exporting countries should communicate freedom of expression standards in all dialogues with all governments.[30]

- Importing countries should publish and follow rights-respecting procedures for bid, procurement, maintenance, and access, and establish civilian oversight and require independent, impartial judicial authorization for use of surveillance technology.
- Export controls can be used to limit and regulate the sale of technology for dual-use surveillance items. This category of so called "dual-use" technology has increasingly been employed to violate human rights around the world (for instance by compromising secure communications channels), but regulating it requires a delicate regulatory balance. As the term dual-use implies, technology in this category often has legitimate uses, as well as harmful ones. Often, the same technologies which underlie surveillance systems can support the development and security of IT infrastructures.
- Over the past years, news reports have revealed that spyware from US, Israel or European-owned firms are being used to target human rights defenders, journalists, and opposition leaders. Access Now helped with one investigation of an attack that deployed malicious messages to snare Mexican public health advocates with malware.[31]
- In 2017, we brought evidence of these attacks to the attention of world governments reviewing the human rights records of the United Arab Emirates and Israel through the UPR process.[32]

ii) Business enterprises' internal safeguards and remedial mechanisms.

- Several large-scale attacks over the past few years, such as the devastating WannaCry attack, were conducted by leveraging vulnerabilities that governments already knew about but kept secret, to stockpile for use against adversaries.
- A vulnerability is a flaw in the technical design or implementation of information technology products or systems that could be used to exploit or penetrate a product or system, either hardware or software.[33] Vulnerabilities of either type are common and will always exist; ensuring that there is an environment which enables their disclosure (and therefore subsequent patching) is of utmost importance.
- Access Now advocate that governments not only have a vulnerability disclosure process for when they find or become aware of technology flaws, but also that governments facilitate coordinated vulnerability disclosure (CVD) within their jurisdiction. This includes making changes that support disclosure and patching of vulnerabilities, such as avoiding criminalising security research and instead giving leeway to prosecutors in related cases.[34]

---

[30] *Supra note 28.*

[31] *Spyware in Mexico: An Interview with Luis Fernando Garcia f R3D Mexico*, Deji Olukotun, https://www.accessnow.org/spyware-mexico-interview-luis-fernando-garcia-r3d-mexico/.

[32] *Supra note 17.*

[33] *The Cert Guide to Coordinate Vulnerability Disclosure*, Carnegie Mellon University Software Engineering Institute, https://resources.sei.cmu.edu/asset_files/SpecialReport/2017_003_001_503340.pdf.

[34] *Recommendations from a Report of CEPS Task Force, Software Vulnerability Disclosure in Europea, Technology Policies, and Legal Challenges*, CEPS Task Force on Software Vulnerability Disclosure in Europe, https://www.ceps.eu/system/files/SVD-%20Flyer%20event%2027%2002%20Parliament-%2024%2002_Final.pdf.

3) *Encryption and anonymity as enablers for the enjoyment of human rights, including the right to freedom of expression and of opinion; challenges raised by encryption and anonymity and ways to address these challenges.*

- Encryption and anonymity, and the security concepts behind them, provide the privacy and security necessary for the exercise of the right to freedom of opinion and expression in the digital age.[35] Such security may be essential for the exercise of other rights, including economic rights, privacy, due process, freedom of peaceful assembly and association, and the right to life and bodily integrity.

i) Encryption

- Encryption has regularly been under attack. Law enforcement officials and legislators argue that encryption has allowed private actors to evade detection. They allege that people should be willing to sacrifice users' security in order for police to expand their investigative capacity.[36] Countries are looking for backdoors to encryption technology. For instance, the United Kingdom passed the Investigatory Powers Act and mandates that technology companies assist government in decrypting information where feasible.[37] With the same objective, Russia passed the Federal Security Service in 2016, a law which require companies to share its encryption keys with the Russian government.
- Unfortunately, an increasing number of states are looking to weaken the use of encryption technology, the Australian Prime Minister stated that his government wants to introduce a method of intercepting and reading encrypted messages, under the presence of keeping the public space from terrorism.[38] Similarly, in the spring of 2016, the Hungarian government introduced a bill as part of a counterterrorism package that included up to two years imprisonment for using encrypted services or providing such services, in addition to mandating backdoors. While the adopted bill did not include these measures, we expect comparable proposals to continue to emerge.
- To counter this trend, Access Now launched a global coalition together with organisations, companies, and experts from around the world at securetheinternet.org — an open letter to world leaders asking for them to support encryption and to avoid mandates that would undermine the security of users and companies.[39] The letter, which has already been signed by more than 250 organisations, individuals,

---

[35] *Europol Supports Encryption. We Can Relax Now… Right?*, Lucie Krahulcova, https://www.accessnow.org/europol-supports-encryption-can-relax-now-right/.
[36] *Id.*
[37] *UK Government Can Force Encryption Removals, but Fears Losing, Experts Say*, Alex Hern, https://www.theguardian.com/technology/2017/mar/29/uk-government-encryption-whatsapp-investigatory-powers-act.
[38] *Strong Enryption Serves Australia's National Interests and Creates More Robust Systems*, Access Now, https://www.accessnow.org/strong-encryption-serves-australias-national-interests-creates-robust-systems/.
[39] *Announcing a global coalition demanding security for all,* Access Now. https://www.accessnow.org/announcing-a-global-coalition-demanding-security-for-all/.

trade associations, and companies, represents a global effort to advance digital security.[40] Organisations that have signed on to the letter hail from over 60 different countries across the world, including Australia, Brazil, India, Mongolia, Myanmar, Turkey, and Zimbabwe. **Access Now encourages governments and decision-makers around the world to endorse this letter.**

- Companies are often unable to successfully defend against backdoor regulations and failure to comply in some instance may lead to the arrest of their employees. For instance a senior Facebook executive in Sao Paulo was detained after the company informed the Brazilian government that Facebook was unable to intercept WhatsApp chats.[41]
- We note that states' efforts to weaken encryption give law enforcement and intelligence services significant power to conduct surveillance.[42]
- Encryption remains a security solution and while proposal to undermine this technology continues to flourish, there is no such thing as creating vulnerabilities of backdoor "just for the good guys". In 2018, Access Now released a report that **concludes that any policy mandating backdoors into encrypted products would likely be effective for only a minimal time**, would be substantially costly, and might **harm security** in general.[43]

ii) Anonymity

- Encryption and anonymity, separately or together, create a zone of privacy to protect opinion and belief. Encryption and anonymity provide individuals and groups with a zone of privacy online to develop and hold opinions and exercise freedom of expression without arbitrary and unlawful interference or attacks.[44]
- Anonymity is key to the enjoyment and exercise of human rights online. By protecting their identity and privacy, vulnerable and marginalised groups can express themselves and raise awareness to their issues.[45]
- Policies forcing online users to reveal their legal or given names -- often called "real" names -- have harmful impacts on sexual, religious, and ethnic minorities, as well as journalists and indigenous peoples. In 2015, Access Now convened the Nameless coalition to push back against Facebook "real name" policy.[46]

---

[40] *Security for all.* https://www.securetheinternet.org/.
[41] *Senior Facebook Executive Arrested in Brazil After Police are Denied Access to Data*, Dom Phillips and Ellen Nakashima https://www.washingtonpost.com/world/national-security/senior-facebook-executive-arrested-in-brazil-after-police-denied-access-to-data/2016/03/01/f66d114c-dfe5-11e5-9c36-e1902f6b6571_story.html?utm_term=.917d1ad57e64.
[42] *The Role of Encryption in Australia A Memorandum*, Access Now, https://www.accessnow.org/cms/assets/uploads/2018/01/Crypto-Australia-Memo.pdf.
[43] *Supra note 33.*
[44] *A/HRC/29/32 - Report of the Special Rapporteur on freedom of expression,* Human Rights Council http://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/CallForSubmission.aspx.
[45] *Nameless Coalition Calls on Facebook to Change its Real Name Policy*, Peter Micek, https://www.accessnow.org/nameless-coalition-calls-on-facebook-to-change-its-real-name-policy/.
[46] *Id.* For examples where real name policies have caused adverse human rights impacts, see, *Appendix to October 5, 2015 Coalition Letter to Facebook* https://www.eff.org/document/appendix-october-5-2015-coalition-letter-facebook.

4) ***National legislative and regulatory frameworks concerning the collection, processing, retention or use of personal data by Governments and other actors, in particular business enterprises, related human rights protection gaps and ways to bridge those gaps.***

Protection of the rights to privacy and personal data

- In 2018, 70 United Nations member states still lack domestic privacy laws and 80% of these states do not have proper laws against disproportionate or arbitrary domestic surveillance.[47] Protecting privacy, in the digital age, means developing comprehensive legal framework for the protection of this right and as well as binding substantive and procedural safeguards on the use of targeted, legitimate, necessary, and proportionate surveillance.
- In addition to the right to privacy, the interconnected **right to protection of personal data should be protected**. While the right to privacy protects an individual's identity, home or beliefs, the right to protection of personal data protects the information that can identify a person's identify, home or beliefs.
- The first data protection law was passed in 1970 by the German federal state of Hesse. A few years later, the U.S. developed "fair information practices" that have largely influenced modern data protection laws — though the U.S. have yet to follow up with a fully comprehensive legal framework for data protection at the federal level. In 1980, the Convention for the protection of individuals with regard to automatic processing of personal data - also known as Convention 108 - was adopted by the Council of Europe. Since its adoption, the convention was ratified by 51 countries. The Convention paves the way for the adoption of modern data protection legislation around the world and today, many countries have adopted general or sectoral data protection laws.[48]
- In the European Union, data protection is a fundamental right, and the General Data Protection Regulation (GDPR) and the Police Directive constitute the new framework for protecting that right. Countries including Tunisia, Japan, Argentina, Australia, Jamaica are considering new data protection laws or upgrading their existing legal frameworks on the basis of the EU reform. Additionally, an expert committee in India is currently deliberating on a data protection and privacy regime for the next billion users of the internet. Notably missing from the list of countries creating a federal framework for data protection is the US, where many leading technology companies are headquartered.
- Since 2017, the EU is negotiating the reform of its privacy law - the ePrivacy Directive - to adapt it to the digital age. The discussions are however challenging as several EU states are seeking to limit or undermine the reform, thus putting at risks protection for the right to privacy and the confidentiality of communications.[49]

Data Retention

---

[47] *A/HRC/37/62 - Report of the Special Rapporteur on the Right to Privacy,* Human Rights Council http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session37/Documents/A_HRC_37_62_EN.docx.

[48] *Supra note 3*.

[49] *Open Letter to European Member States on ePrivacy Reform*, https://www.accessnow.org/cms/assets/uploads/2018/03/ePrivacy-openletter-FINAL.pdf.

- Countries around the world are looking to expand their surveillance power by implementing legislations that impose longer data retention periods and increase disclosure to state actors. For instance, in August 2017, the Chilean Ministry of Internal Affairs and Public Security issued Decree 866 of the Code of Criminal Procedure. The decree requires all internet service providers to retain IP address information showing the websites visited — including the date, time, and duration of the visit — for one year, and must make these records available for the judiciary. The objective of mandatory data retention is to create a massive, disproportionate surveillance mechanism for the web browsing activity of millions of people, not because they are under suspicion for any crime, but "just in case."[50]
- International courts have deemed that **general data retention mandates fails to comport with the necessity and proportionality principles and violate international human rights standards**. For instance, in 2014, the Court of Justice of the European Union overturned the Data Retention Directive, which required that all telecommunications data be indiscriminately collected and retained by providers for a minimum and maximum of six months up to two years, respectively.[51] The court in this case held that blanket data retention legislation are incompatible with Article 7 and 8 of the European Charter of Fundamental Rights - respectively protecting the rights to privacy and data protection. Specifically, the court found that data retention provisions should be strictly limited to those that are "directly suspect or tangibly linked to serious crime, and the retention is permissible only for the period that the crime is under investigation." It also further clarified the criteria limiting the use of data retention in a 2016 ruling.[52]
- Despite these courts rulings, most EU states continue to have general data retention laws which fail to comply with the standards established by the EU Court and thus neglect the rights to privacy and data protection.[53]
- Similarly, Latin American countries, including Mexico, Colombia, and Brazil, are moving towards blanket data retention mandates.[54]

Companies practices

- Companies' processing of personal information or **use of invasive techniques such as tracking or profiling is constantly increasing to the detriment of user's privacy.**
- In October 2014, Access Now launched the AmIBeingTracked.com initiative to enable users of mobile internet access services to determine whether their internet service provider was using "supercookies"

---

[50] *Chile's "Spy Decree" Threatens to Make Data Rentention Even More Dangerous*, Javier Pallero and Veronica Arroyo, https://www.accessnow.org/chiles-spy-decree-threatens-make-data-retention-even-dangerous/.

[51] V*ictory! EU Court Rules That Discriminate Data Retention is not Permissible*, Access Now, https://www.accessnow.org/victory-eu-court-rules-indiscriminate-data-retention-not-permissible/.

[52] *Tele2 Sverige AB v. Post -Och Telestyrelsen*, Judgment of the Court (Grand Chamber), http://curia.europa.eu/juris/document/document.jsf?text=&docid=188001&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=176849.

[53] *A Concerning State of Play for the Right to Privacy in Europe*, National Data Retention Laws Since CJEU's Tele-2/Watson Judgment, Privacy International, https://privacyinternational.org/advocacy-briefing/735/report-national-data-retention-laws-cjeus-tele-2watson-judgment.

[54] *Supra note 43*.

- special tracking headers that the telecoms providers inject beyond the control of the user.[55] After its launch in October 2014, more than 330,000 people used the tool, and the results showed significant and secret global deployment of supercookies. Through this research, we found that carriers in 10 countries around the world, including in Canada, China, India, Mexico, Morocco, Peru, the Netherlands, Spain, the US, and Venezuela, are using tracking headers. We also found information indicating the use of tracking headers date back 15 years and that the use of the "Do not track" tools in web browsers did not block or prevent the tracking headers injected by the telcos in question. In 2016, the US Federal Communications Commission fined Verizon for inserting these tracking headers without user permission.

- The recent Facebook/Cambridge Analytica incident illustrate the foreseeable consequence of a common business model: the widespread over-collection and use of personal information to create profiles of users, in particular to generate better ad targeting.[56] Together with a coalition of organisations, Access Now wrote to the EU member states to express that this scandal shows that trust-corrosive practices must be tackled through **robust, binding and enforceable rules on privacy**.[57] The societal implications are profound as this case is further proof that when individuals are tracked and profiled, not only is their privacy at risk, but information can be used for political and economic manipulation.
- This is not the first time that companies, like Facebook, misuse personal data to the detriment of end users.[58] Reports of these types of incidents go back years, and range from third-party abuse to damaging social experiments. A large number of advocates and researchers have warned about possible misuse of Facebook for years.
- Social media companies are not the only private entities targeting and profiling users. Security firms like Gemalto or Safran design services and products that government can use for border surveillance, through Passenger Name Record, Digital ID or Smart Border systems. In some cases, these companies are also closely linked with decision-makers in charge of adopting legislation that will require the use of their products.[59]
- Finally, all around the world data brokers, like Palantir or Acxiom, monetize user information by amassing user data, and extrapolating inferences about individuals which are organised to create profiles. These profiles are then sold and used for a variety of commercial or non-commercial purposes. Users do not know how companies are profiling their activities, or even that sort of speculations ar made. The information data brokers use to create profiles includes public information, content that

[55] *The Rise of Mobile Tracking Headers: How Telcos Around the World Are Threatening Your Privacy*, Access Now, https://www.accessnow.org/cms/assets/uploads/archive/AIBT-Report.pdf. See FCC action against Verizon here: https://www.theverge.com/2016/3/7/11173010/verizon-supercookie-fine-1-3-million-fcc

[56] *Supra note 4*.

[57] *Supra note 42*.

[58] *Supra note 4*.

[59] *The Curious Tale of The French Prime Minister, PNR and Peculiar Patterns*, Estelle Massé and Joe McNamee,https://www.euractiv.com/section/justice-home-affairs/opinion/checked-for-tuesthe-curious-tale-of-the-french-prime-minister-pnr-and-peculiar-patterns/.

users choose to share publicly but also information that users generate without necessarily being aware through the digital footprint.[60]

- There is a crucial need to **enforce data protection privacy and transparency obligations on security firms and data brokers** given the significant impacts of their activities on the privacy of individuals.

5) *Growing reliance on data-driven technology and biometric data:*

a) *How can new technologies help promote and protect the right to privacy?*
b) *What are the main challenges regarding the impact on the right to privacy and other human rights?*
c) *What are the avenues for adequate protection of the right to privacy against threats created by those technologies? How can the international community, including the UN, address human rights challenges arising in the context of new and emerging digital technology*

- **Access Now believe that users' rights should be placed at the centre of innovation and development.** Today's data driven society is beginning to raise many questions about the impact of data and its misuse. With the rise of the Internet of Things and Artificial Intelligence, the challenges to the right to privacy will acutely intensify.
- Companies have a responsibility both to know about the impact of their products and services on human rights, by conducting due diligence, working with outside stakeholders, and taking measures to prevent and mitigate any adverse effects. **Access Now recommends public and private sector entities to abide by the principles of security, data protection and privacy by design.**
- In addition, companies have international obligations to prevent, mitigate, and provide redress when human rights are violated – and this includes the right to privacy.[61]
- On the other hand, **governments have a responsibility to strengthen data protection and privacy laws** when they exists. In countries where a data protection framework is missing or insufficient — like the US or India — it is time to start building. Based on our experience engaging with lawmakers in Europe on drafting the General Data Protection Regulation, Access Now developed a guide with do's and don'ts for building a data protection framework.[62]
- As regards biometric information, this category of sensitive data include fingerprints, DNA, signatures, retina, iris and vein patterns, facial geometry, or even voice patterns. Biometric data is vulnerable to hacking just like other authentication methods, but unlike a password, biometric indicators cannot simply be reset as needed. This is why the use of biometric data poses significant privacy and security risks.

---

[60] *FTC Data Broker Report Higlights Lack Of Transparency, Calls for Legislative Reform*, Brianna Lazerwitz, https://www.accessnow.org/ftc-data-broker-report-highlights-lack-of-transparency-calls-for-legislativ/.
[61] *United Nations Guiding Principles on Business and Human Rights - Implementing the United Nations "Protect, Respect, and Remedy" Framework*, http://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf.
[62] *Data Protection: Why it Matter and How to Protect It,* Estelle Massé, https://www.accessnow.org/data-protection-matters-protect/.

- Biometric data have become increasingly popular in the public and private sectors as a means of identifying individuals and providing an alternate pathway for user authentication. Governments around the world, including in India and Tunisia are also considering proposal for unique ID or digital ID which includes the collection of biometric data.
- Access Now have developed a draft policy paper, which examines national digital identity programmes from a human rights perspective.[63] Given the potential for exploitation of biometric data, we **discourage the use of these data in digital identify programmes** and propose safeguards and policy recommendations. For instance, we recommend **avoiding the creation of centralised databases of individuals' biometric data**. Given the sensitivity of biometric information, and the fact that "restorability" is limited or impossible when information is compromised, we advise ensuring that such data are stored in a decentralised manner. A centralised database is more vulnerable, since it creates a single point of failure.

6) *Undue interference with the right to privacy in the digital age that may have particular effects on vulnerable or marginalized groups, and based on a person's perceived gender, age, religion, sexual orientation, and other characteristics.*

- Access Now's mission is to defend and extend the digital rights of users a*t risk* around the world. Access Now's Digital Security Helpline particularly works with individuals and organisations around the world to keep them safe online. Since 2013, Access Now's Digital Security Helpline has handled over 166 cases for groups or individuals that defend women's rights. Around half of these clients requested security consultations and sought advice on protecting the privacy of their communications. For the past two years, the most common requests to our Helpline from these groups have been for assistance with compromised or potentially compromised accounts; harassment incidents; and secure communication.
- As noted above, the need of online anonymity is particularly important for users at risk, who are often victimised because - among other things - their affiliation to minority groups or due to their political opinions. Company policies like Facebook's "authentic name", requires users to provide their real name and information to use the service. Previously, when people use pseudonyms and are flagged, the company has unilaterally altered the name on accounts to the legal name. This company poses a significant risk to activists. As noted by "La Gringa" Honduran blogger, " [t]his week I started writing a series of blog articles about crime and narco trafficking in Honduras — and it is likely what prompted the complaint about my account, just as posting of my political articles were blocked by Facebook for a time last year and the year before because of a false complaint […] By asking for a copy of my ID, Facebook is asking me to put my life in danger. By disabling my account, Facebook is silencing one of the few internet voices in English in Honduras."
- Through our work, **we have witnessed how vulnerable groups, marginalised populations and minorities are often the first and most significantly impacted by ill-conceived policies**. For instance, if automated algorithmic solutions fail to integrate important human context, human rights and thus increase and institutionalised discrimination. Decisions from algorithms - whether in the field of human resources,

[63] *National Digital Identity Programmes: What's Next? Final Draft for Comments*, Access Now, https://www.accessnow.org/cms/assets/uploads/2018/03/Digital-Identity-Paper-digital-version-Mar20.pdf.

criminal justice or health - often put population at risks including women, LGBTQI people, activists, journalists and ethnic, religious and political minorities.[64]

- With the development of artificial intelligence and machine learning, these issues will exacerbate. To function, artificial intelligence inherently relies on gathering large amounts of data, and often on the creation of new datasets - so called Big Data - that can be used to make assumptions about people. These practices interfere with the fundamental rights to privacy and data protection. Through binding privacy and data protection frameworks, **governments should provide a right to information, a right to object and a right to explanation linked to the use of algorithms and AI.**[65] Some risks could further be mitigated by developing a sustainable use of these technologies grounded on human rights frameworks, by including mechanism for algorithmic transparency and accountability and by ensuring that developers acknowledge their own biases and work in diverse teams.

7) *Procedural and institutional safeguards, oversight mechanisms and remedies available to individuals exposed to domestic or extraterritorial surveillance, the interception of digital communications or other forms of processing of personal data by governments, business enterprises or private organisations.*

- In the digital age, information about users travel across borders, therefore their rights should be respected at all time: **the universality of the right to privacy, recognised in UN and regional instruments, must be implemented at the state level.**
- Access Now calls for a ban of government mass surveillance which relies on practices contrary to international human rights framework, in particular the right to privacy, and fails to meet the necessary and proportionate standard for restrictions on that right.
- **Access Now recommends that states** developing domestic or extraterritorial surveillance **apply the International Principles on the Application of Human Rights to Communications Surveillance. Known as "the necessary and proportionate" principles**, they attempt to clarify how international human rights law applies in the digital environment, particularly in light of the increase in and changes to surveillance technologies and techniques.[66] In particular, these principles recommend states develop avenues for remedy, increased safeguards, and independent oversight.
- These principles were recognised in the report "the right to privacy in the digital age" issued by the United Nations Office of the High Commissioner for Human Rights as the result of a UN General Assembly resolution from December 2013 addressing global concern about government surveillance activities around the world and their chilling impact on human rights.[67] In 2015, Access Now released an Implementation Guide for the International Principles on the Application of Human Rights to Communications Surveillance. The Implementation Guide applies the

[64] *Machine Bias - There's Software Used Across the Country to Predict Future Criminals. And it's Biased Against Blacks*, Julia Angwin, Jeff Larson, Surya Mattu and Lauren Kirchner, https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing.

[65] *Artificial Intelligence: What are the Issues for Digital Rights*, Estelle Massé and Fanny Hidvégi, https://www.accessnow.org/artificial-intelligence-issues-digital-rights/.

[66] *Necessary & Proportionate - International Principles on the Application of Human RIghts to Communications Surveillance*, https://necessaryandproportionate.org/principles.

[67] *A/HRC/27/37 - Report of the Office of the United Nations High Commissioner for Human Rights,* Human Rights Council http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf.

Principles to each step of the government surveillance process, calling on officials to respect human rights no matter the justification for the activity — whether it is law enforcement, national security, or intelligence gathering.[68]

- Finally, **users and organisations must have the ability to challenge the validity of surveillance laws and their compliance with human rights in front of courts**. In the European Union, while many states have far-reaching extraterritorial surveillance laws, governments continue to argue that users cannot challenge these laws in front of the Court of Justice of the EU. The reasoning for this is that, according to the EU treaties, public security and defense remain an exclusive competence of the states and thus the EU cannot decide on that matters. At the same time, EU states have been successfully pressuring the EU for several years now to adopt legislation that establish surveillance programmes across the EU - such as the now invalid Data Retention Directive or the EU Passenger Name Record Directive. The EU should stop this double game and **allow users to seek remedy for surveillance measures applied by states which impact their right to privacy in accordance with the EU Charter of Fundamental Rights**. On the other hand, EU member states, as part of the Council of Europe framework, are also signatories to the European Convention on Human Rights which is enforced by the European Court of Human Rights.[69]

Conclusion

The protection of the right to privacy in the digital age is central to the enjoyment and exercise of human rights online and offline. Access Now is thankful for the opportunity provided by the United Nations Office of the High Commissioner for Human Rights to input into the upcoming report, and look forward to future engagement.

***

For more information, please visit www.accessnow.org ***and contact:***
Peter Micek, General Counsel | peter@accessnow.org
Fanny Hidvégi, European Policy Manager | fanny@accessnow.org
Estelle Massé, Senior Policy Analyst | estelle@accessnow.org
Denis Nolasco, | denis@accessnow.org

[68] *Universal Implementation Guide for the International Principles on the Application of Human Rights to Communications Surveillance*, Access Now, https://www.accessnow.org/cms/assets/uploads/archive/Implementation%20Guide%20International%20Principles%202015.pdf.

[69] *The court's legal standard and its jurisprudence is analysed in more details in section 2.ii of this submission.*