Access Now submission to the United Nations Human Rights Council, on the Universal Periodic Review 2016 Cycle for the United Kingdom

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 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 good security policies that protect user rights, including privacy and freedom of expression. Access Now has worked extensively in Europe and the UK on digital rights.
3. This is the third review for the United Kingdom, last reviewed in May 2012, at the Universal Periodic Review Mechanism (UPRM) in Geneva.

Domestic and international human rights obligations

4. The UK has signed onto various international human rights instruments, including the International Covenant on Civil and Political Rights (ICCPR), the Convention against Torture (CAT), and the Optional Protocol to the CAT (OPCAT).
5. The UK is also currently party to the European Convention on Human Rights (ECHR). In her former position as Home Secretary, current Prime Minister Theresa May promoted the UK's withdrawal from the ECHR and the jurisdiction of the European Court of Human Rights.

Situation of digital rights in the United Kingdom

7. Despite these commitments and obligations, we have gathered and hereby submit evidence of disregard of digital rights in the United Kingdom. These violations include:

Violations of the right to freedom of expression and opinion

8. Encryption protects the confidentiality and integrity of communications, creating a "zone online to hold opinions and exercise freedom of expression without arbitrary and unlawful interference or attacks."[1] In reporting on the connection, the United Nations Special Rapporteur for the Promotion and Protection of the Right to Freedom of Opinion and Expression found that "[e]ncryption and anonymity, today's leading vehicles for

[1] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Human Rights Council, U.N. Doc.A/HRC/29/32 at 3, 6 (May 22, 2015) (by David Kaye).

online security, provide individuals with a means to protect their privacy, empowering them to browse, read, develop and share opinions and information without interference and enabling journalists, civil society organisations, members of ethnic or religious groups, those persecuted because of their sexual orientation or gender identity, activists, scholars, artists and others to exercise the rights to freedom of opinion and expression" and limitations on encryption must be in conformity with human rights.

9. The pending Investigatory Powers Bill (IP Bill) creates ambiguity as to the power of the Secretary of State to regulate encryption, particularly whether regulations to be developed under §217 on "technical capability notices" could enable limitations on the use or development of strong encryption or the requirement to implement encryption backdoors.[2] Such requirements would have a direct, deleterious impact on digital security.
10. Further, uncertainty under the law and future regulations would lead to an underdevelopment of security measures. If encryption is weakened, users will lose trust in the security of the internet and modify their behavior accordingly. They may limit sharing of sensitive information or cease trusting security patches. These risks are aggravated by the geographic scope of technical capability notices, which can be given to a person inside or outside the UK.[3]

Violations of the right to privacy

8. The UK High Court has held the Data Retention and Investigatory Powers Act of 2014 (DRIPA) violates EU law.[4] United Kingdom civil liberties groups and individual Members of Parliament brought the case. Previously, the Court of Justice of the European Union ("CJEU") had struck down the EU Data Retention Directive in 2014 because it created a disproportionate interference with the fundamental rights to respect for private life.[5]
9. *A priori* data retention requirements, which create an undue burden on business, risk data security, infringe upon individual privacy, and chill the exercise of human rights including freedom of expression and freedom of association.[6] Human rights violations are particularly pronounced in legislation such as DRIPA, which are devoid of meaningful limits to the scope of the data that provider can be compelled to retain.
10. The UK has continued to enforce *a priori* data retention requirements on operators. The Parliament is currently considering the Investigatory Powers Bill that, if passed, will continue to oblige providers to retain user data.

---

[2] Draft IP Bill §§ 217(4)(c) ("The obligations that may be specified in regulations under this section include, among other things- . . . obligations relating to the removal by a relevant operator of electronic protection applied by or on behalf of that operator to any communications").
[3] Draft IP Bill §§ 218(11)(b).
[4] https://www.judiciary.gov.uk/wp-content/uploads/2015/07/davis_judgment.pdf
[5] *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others* (C-293/12), available at http://curia.europa.eu/juris/liste.jsf?num=C-293/12.
[6] International Principles on the Application of Human Rights to Communications Surveillance, https://necessaryandproportionate.org.

11. The UK has served as a host to companies producing, marketing, and exporting invasive surveillance technologies without adequate safeguards against abuse. Technologies such as FinFisher, a suite of trojan based systems formerly exported by UK-based Gamma International, were being exported to authoritarian states with poor human rights records and being used to target activists.[7] The fact that such technology can be used to target individuals across borders – as well as within the UK itself[8] -- necessitates strict controls and human rights safeguards to prevent misuse or abuse, including by governments known for systematic infringement of human rights.

Recommendations

12. The United Kingdom can improve its human rights record and treatment of digital rights in several areas. We accordingly recommend that the government of the United Kingdom:
    a. Commit to enhancing freedom of expression online and preventing violations by state and non-state actors, such as companies;
    b. Improve cooperation with United Nations treaty mechanisms and issue standing invitations to UN special procedures such as the UN special rapporteurs on freedom of expression and privacy;
    c. Commit to protecting the use of strong encryption by codifying protections in conformity with the report by Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression David Kaye on the use of encryption and anonymity in digital communications;
    d. Commit to upholding EU human rights obligations and ensuring effective remedy for violations of human rights regardless of future political status by remaining a party of the ECHR and thus continuing to submit to the jurisdiction of the ECtHR.
    e. Enact laws protecting access to information and preventing network discrimination, also known as Net Neutrality.
13. 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.
14. For additional information, please contact Access Now staff member Peter Micek (peter@accessnow.org).

---

[7] http://www.bloomberg.com/news/articles/2012-07-25/cyber-attacks-on-activists-traced-to-finfisher-spyware-of-gamma

[8] https://www.privacyinternational.org/?q=node/84