Foreign & Commonwealth Office

Submission to the Office of the High Commissioner for Human Rights: The right to privacy in the digital age

United Kingdom of Great Britain and Northern Ireland, April 2018

The United Kingdom of Great Britain and Northern Ireland welcomes the opportunity to provide input to the Office of the High Commissioner for Human Rights on human rights challenges relating to the right to privacy in the digital age, including on principles, standards and best practices with regard to the promotion and protection of the right to privacy.

The rise of digital communications and technologies has opened up many opportunities for people to communicate and do business. We recognise that these opportunities have led to concerns over privacy and data protection, and we acknowledge our obligation to safeguard our citizens, their right to freedom of expression and to privacy. The United Kingdom co-sponsored the 2012, 2014 and 2016 UN Human Rights Council resolutions on the protection, promotion and enjoyment of human rights on the internet. In accordance with those resolutions, we continue to affirm that the same rights people have offline must be protected online. The United Kingdom has also supported Human Rights Council and General Assembly resolutions on the right to privacy in the digital age.

Surveillance and communications interception

The United Kingdom has an obligation to ensure the safety and security of its citizens. However, we believe that this obligation does not in any way detract from the obligation to protect human rights. States can and should deliver both privacy and security both offline and online.

We believe that states should be transparent about their powers for surveillance and communications interception, and develop and implement appropriate safeguards. In the United Kingdom, we recently overhauled our domestic investigatory powers legislation, resulting in the Investigatory Powers Act 2016. The Investigatory Powers Act provides world-leading transparency and privacy protections, including an overarching clause that sets out the privacy considerations that must be taken into account before issuing any warrant, authorisation or notice under the Act.

The Act requires all conduct to be necessary, proportionate, and carried out in accordance with the Human Rights Act, ensuring that arbitrary use of the powers is unlawful. It introduces judicial authorisation for the most intrusive powers, and includes specific additional protections for more sensitive categories of data such as journalistic material. It also creates the powerful new office of the Investigatory Powers Commissioner (IPC). The IPC, a senior judge, is responsible for the independent oversight of public authorities' use of investigatory powers. They can call on expert legal and technical advice, and can require the disclosure to them of any information relevant to their oversight, including by the security and intelligence agencies.

The Act also contains provisions relating to encryption. The United Kingdom is in favour of strong encryption: it is critical to protect UK citizens from harm online and billions of people use encryption every day. We do not want unfettered access to all communications. However, in tightly proscribed circumstances, the United Kingdom's law enforcement and security and intelligence agencies must be able to access the communications of criminals, including terrorists, where there is a warrant authorised by a Secretary of State and approved by a judge.

We recognise that encryption can serve a particularly vital purpose to protect journalists, human rights defenders and other vulnerable people. The United Kingdom has funded the training and deployment of encryption overseas: for instance, supporting human rights defenders to draw attention to violations and abuses.

Sale of surveillance technology

The United Kingdom supports appropriate controls on the sale of surveillance technology that could pose risks to human rights, and was instrumental in getting agreement in the Wassenaar Arrangement for controls on intrusion software tools. However any controls must be proportionate, be able to be applied effectively, and must not impose unnecessary burdens on legitimate trade.

Risks around human rights violations are a key part of assessments. The United Kingdom does not export equipment where we assess there is a clear risk that it might be used for internal repression, or would provoke or prolong conflict within a country, or would be used aggressively against another country. All export licence applications are considered on a case-by-case basis against the Consolidated EU and National Arms Export Licensing Criteria (the 'Consolidated Criteria') based on the most up-to-date information and analysis available, including reports from NGOs and our overseas network. These are not decisions that the United Kingdom takes lightly and we will not license the export of items where to do so would be inconsistent with any provision of the Consolidated Criteria, including where we assess there is a clear risk that the goods may be used for internal repression.

Data protection

In recognition of the need for robust data protection, a new Data Protection Bill was introduced in Parliament in September 2017. The Bill is intended to create a new data protection framework fit for the digital age, which incorporates the provisions of the EU's General Data Protection Regulation (GDPR) and Data Protection Directive (DPD) into

domestic law. In particular, the Bill builds on existing standards for protecting personal data, in accordance with the GDPR, giving people more control over the use of their data and providing new rights to move or delete personal data.

Data subjects will benefit from a range of new rights, including easier access to their data; the right to information on how their data has been processed free of charge; the right to be made aware of a breach concerning their data; and a requirement on controllers to carry out data protection impact assessments where processing is likely to result in a high risk to the rights and freedoms of a data subject.

The United Kingdom will continue to play a leading global role in the development and promotion of appropriate data protection standards and cross-border data flows, working with international partners to ensure that data protection standards are fit for purpose – both to protect the rights of individuals, but also to allow businesses and public authorities to offer effective services and protect the public.