Joint Civil Society Statement on Encryption

We, the undersigned human rights, freedom of expression and civil society organisations, are deeply concerned about government proposals to undermine the use of encryption on online platforms and messaging services. The recent statement of the Five Eyes governments, with India and Japan, calls upon these platforms and messaging services to enable access by law enforcement agencies to private communications protected by end-to-end encrypted communication. And the UK government is even considering, through its Online Harms Bill, to require companies to monitor private communications themselves to identify “harmful content”.

Encryption, and end-to-end encryption in particular, provides a guarantee that our private communications and information will be secure, and not vulnerable to being hacked or otherwise accessed without our consent. While we recognise the challenges that encryption brings, it is a technology that millions of people across the world rely upon for their privacy, safety and security. For some of the most persecuted in the world, their very physical safety depends on their ability to be able to communicate privately and securely.

Journalists, human rights defenders, whistle-blowers, activists, and minorities vulnerable to persecution rely upon the security that encryption provides in order to exercise their human rights to freedom of expression, freedom of information, and association and assembly. Investigative journalists particularly rely on encryption to guarantee source protection and inform their public interest reporting - directly impacting the public’s right to information.

In the UK, we rely upon the privacy and security that encryption provides every day, to keep our communications, personal information, and online interactions secure from hackers and data breaches. The ability to be able to send and receive messages in the knowledge that they will be kept private is something that the British public care deeply about. In a recent survey, only 29% of the public stated that they felt comfortable with companies being able to access private messages to try and identify illegal or harmful content, compared to 52% who said that they were uncomfortable about this.

The importance of the availability of strong encryption has also been recognised by human rights bodies and experts around the world. These include not only UN Special Rapporteurs, but the UN Human Rights Council and the Freedom Online Coalition, both bodies of which the UK is a member. Instead of attacking or seeking to undermine the use of encryption, the UK government should be living up to its international commitments, defending and promoting its use as a critical means for ensuring privacy and cybersecurity, and the rights to freedom of expression and freedom of information.

There is a near universal consensus among technologists that there is simply no way that encryption can be weakened only for malicious actors. Any intentional undermining of compromising of encryption, even for legitimate purposes, weakens everyone's security online. And to require companies to remove the protections provided by encryption so that they themselves can monitor our private messages would create a degree of surveillance that should not be tolerated in a democratic society.

We therefore call upon the government:

- To ensure that the Online Harms Bill, and any duty of care or codes of practices established through the legislation:
    - do not require or encourage companies to compromise their use of encryption;
    - do not place any conditions, or impose any additional potential liability, on an online platform in connection with its use of encryption; and
    - include explicit exemptions for encrypted and private communications;
- To use alternative methods of investigation, including existing capabilities and powers, to identify illegal behaviour online, provided that they comply with the UK's international and national human rights obligations; and
- To cease other efforts to weaken or undermine encryption beyond the scope of the Online Harms Bill, including the creation of backdoors or establishing a ghost user presence in specific encryption tools.
- To promote the use of strong encryption nationally and internationally, as a critical element of privacy and security, and particularly in countries and contexts where people's safety would otherwise be put at risk.

Signatories

- ARTICLE 19
- Big Brother Watch
- English PEN
- Global Partners Digital
- Index on Censorship
- Open Rights Group
- Privacy International
- Reporters Without Borders (RSF)
- Scottish PEN