Deeply Flawed Censorship Project: Experts Condemn UK Online Safety Bill as Harmful to Privacy and Encryption

By Joe Mullin
Global Research, November 25, 2022
Electronic Frontier Freedom 23 November 2022

Region: Europe
Theme: Law and Justice, Police State & Civil Rights

All Global Research articles can be read in 51 languages by activating the Translate Website button below the author's name.

To receive Global Research's Daily Newsletter (selected articles), click here.

Follow us on Instagram and Twitter and subscribe to our Telegram Channel. Feel free to repost and share widely Global Research articles.

***

The British Parliament may start debating the Online Safety Bill again as soon as this week. The bill is a deeply flawed censorship proposal that would allow U.K. residents to be thrown in jail for what they say online. It would also force online service providers to use government-approved software to search for user content that is deemed to be related to terrorism or child abuse. In the process, it will undermine our right to have a private conversation, and the technologies that protect that right, like end-to-end encryption.

In a letter published today, EFF has joined dozens of security researchers and human rights groups to send a clear message to incoming U.K. prime minister Rishi Sunak: the Online Safety Bill must not undermine encryption. As the letter notes, in its current form, the Online Safety Bill "contains clauses that would erode end-to-end encryption in private messaging." It continues:

> Undermining protections for end-to-end encryption would make UK businesses and individuals less safe online, including the very groups that the Online Safety Bill intends to protect. Furthermore, because the right to privacy and freedom of expression are intertwined, these proposals would undermine freedom of speech, a key characteristic of free societies that differentiate the UK from aggressors that use oppression and coercion to achieve their aims.

In the past few years, we've seen a number of proposals brought forward by governments that want to scan user-to-user communications for criminal content: the U.S. EARN IT Act, and the EU's proposal to scan private chats. All of these proposals suffer from the incorrect belief that a backdoor or other workaround to read encrypted messages can be designed for use only in benevolent ways.

| 1

That [isn't the case](#), and never will be. Criminals, rogue employees, domestic abusers, and authoritarian governments are just some of the bad actors that will eagerly exploit backdoors like those proposed by the Online Safety Bill. Proposals like this threaten a basic human right: our right to have a private conversation.

We hope Prime Minister Sunak acknowledges the consensus among technologists against the current Online Safety Bill and proposals like it.

*

Note to readers: Please click the share buttons above. Follow us on Instagram and Twitter and subscribe to our Telegram Channel. Feel free to repost and share widely Global Research articles.

Featured image is from blogtrepreneur/Flickr

The original source of this article is [Electronic Frontier Freedom](#)
Copyright © [Joe Mullin](#), [Electronic Frontier Freedom](#), 2022

[Comment on Global Research Articles on our Facebook page](#)

[Become a Member of Global Research](#)

Articles by: [Joe Mullin](#)