GlobalResearch
Center for Research on Globalization

Extreme Online Surveillance in the UK: Extreme :"Online Safety Bill" (OSB) Envisages Invasive Scanning of "User Files".

The OSBThe OSB Bill would give the U.K. government the right to order message and photo-scanning, and that will harm the privacy and security of internet users worldwide

By Joe Mullin
Global Research, September 12, 2023
Electronic Frontier Foundation 8 September 2023

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

***

The U.K.'s Online Safety Bill (OSB) has passed a critical final stage in the House of Lords, and envisions a potentially vast scheme to surveil internet users.

The bill would empower the U.K. government, in certain situations, to demand that online platforms use government-approved software to search through all users' photos, files, and messages, scanning for illegal content. Online services that don't comply can be subject to extreme penalties, including criminal penalties.

Such a backdoor scanning system can and will be exploited by bad actors. It will also produce false positives, leading to false accusations of child abuse that will have to be resolved. That's why the OSB is incompatible with end-to-end encryption—and human rights. EFF has strongly opposed this bill from the start.

Now, with the bill on the verge of becoming U.K. law, the **U.K. government has sheepishly acknowledged that it may not be able to make use of some aspects of this law.** During a final debate over the bill, a representative of the government said that **orders to scan user files** "can be issued only where technically feasible," as determined by Ofcom, the U.K.'s telecom regulatory agency. He also said any such order must be compatible with U.K. and European human rights law.

That's a notable step back, since previously the same representative, Lord Parkinson of

Whitley Bay, said in a letter to the House of Lords that the technology that would magically make invasive scanning co-exist with end-to-end encryption *already existed*. "We have seen companies develop such solutions for platforms with end-to-end encryption before," wrote Lord Parkinson in that letter.

Now, Parkinson has come quite close to admitting that such technology does not, in fact, exist. On Tuesday, he said:

> There is no intention by the Government to weaken the encryption technology used by platforms, and we have built strong safeguards into the Bill to ensure that users' privacy is protected.
>
> If appropriate technology which meets these requirements does not exist, Ofcom cannot require its use. That is why the powers include the ability for Ofcom to require companies to make best endeavors to develop or source a new solution.

The same day that these public statements were made, news outlets reported that the U.K. government privately acknowledged that there is no technology that could examine end-to-end encrypted messages while respecting user privacy.

People Need Privacy, Not Weak Promises

Let's be clear: weak statements by government ministers, such as the hedging from Lord Parkinson during this week's debate, are no substitute for real privacy rights.

Nothing in the law's text has changed. **The OSB gives the U.K. government the right to order message and photo-scanning, and that will harm the privacy and security of internet users worldwide**. These powers, enshrined in Clause 122 of the OSB, are now set to become law. After that, the regulator in charge of enforcing the law, Ofcom, will have to devise and publish a set of regulations regarding how the law will be enforced.

Several companies that provide end-to-end encrypted services have said they will withdraw from the U.K. if Ofcom actually takes the extreme choice of requiring examination of currently encrypted messages. Those companies include Meta-owned WhatsApp, Signal, and U.K.-based Element, among others.

While it's the last minute, Members of Parliament still could introduce an amendment with real protections for user privacy, including an explicit protection for real end-to-end encryption.

Failing that, Ofcom should publish regulations that make clear that there is no available technology that can allow for scanning of user data to co-exist with strong encryption and privacy.

Finally, lawmakers in other jurisdictions, including the United States, should take heed of the embarrassing result of passing a law that is not just deceptive, but unhinged from computational reality. The U.K. government has insisted that through software "magic," a system in which they can examine or scan everything will also somehow be a privacy-protecting system. **Faced with the reality of this contradiction, the government has turned to an 11th hour campaign to assure people that the powers it has demanded simply won't be used.**

*

Note to readers: Please click the share button 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 EFF
