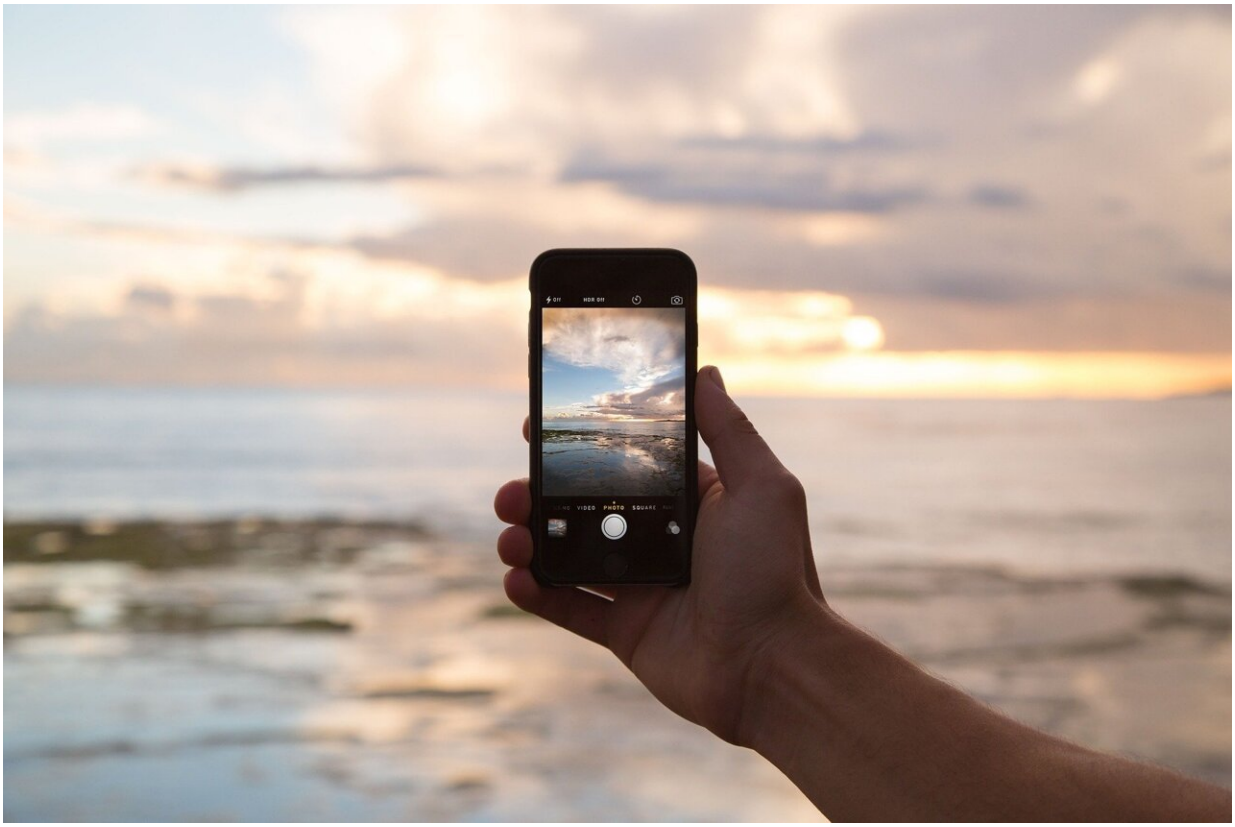
Tech mandated by UK Online Safety Bill 'could turn phones into surveillance tools'

May 19 2023, by Laura Gallagher, Caroline Brogan



Credit: Pixabay/CC0 Public Domain

Tech mandated by the UK Government's Online Safety Bill could be used to turn millions of phones into facial recognition tools.

This is according to new research from Imperial College London that looked at the potential privacy implications of a tool called client-side scanning (CSS). Under the Online Safety Bill, CSS would be introduced to flag when people are trying to share images that are known to be illegal content, such as images of child abuse, before they are encrypted and sent.

The new research shows it would be possible for governments to use CSS to search people's private messages, for example performing facial recognition, without their knowledge.

The Online Safety Bill is currently being reviewed in the UK parliament. CSS is also part of an EU proposal which, if passed, could mandate its installation on hundreds of millions of phones. It has already been developed in the US by companies like Apple.

The new paper is being presented and published next week at IEEE Security and Privacy, one of the leading security conferences in the world. Corresponding author Dr. Yves-Alexandre de Montjoye, of Imperial College London's Department of Computing, said, "This Bill would mandate the installation of software to check you don't share images known to contain child sexual abuse material."

"But what our paper shows is that the software could be built or tweaked to include other hidden features such as scanning private content from the phones of hundreds of millions of people using facial recognition, the same technology used at airport gates."

Illegal online activity

Governments have long been concerned that end-to-end encryption—the function used by messaging apps like WhatsApp and Signal that ensures only the sender and intended recipient of a message can read

it—prevents law enforcement agencies from accessing messages with illegal content.

To tackle this perceived risk, the proposed Bill would mandate apps to install CSS, which would scan images on a phone before they are encrypted and sent.

The software would compare the signature of images of known illegal content from an official database. A 'match' would indicate that the content is known to be illegal and it would be reported and shared with crime agencies, unencrypted.

However, the researchers say that their findings show that we don't understand the risks well enough to mandate their deployment on hundreds of millions of devices.

To carry out the study, the team recreated the algorithms that underpin CSS, to match the signature of images to the database of known illegal content. They then taught the software to also scan the content for wanted faces. They show their software to be indistinguishable from the original one while being very accurate at identifying the faces of wanted persons in people's photos.

Co-author Shubham Jain, also from Imperial's Department of Computing, said, "It's vitally important to tackle illegal content online and we must do so in effective ways. However, CSS threatens to add a backdoor into personal devices, sacrificing the privacy of millions."

Dr. de Montjoye said, "It is our opinion that client-side scanning is not the innocuous 'single purpose' technology it has been described to Parliament as. We call on policymakers to thoroughly evaluate the pros and cons of client-side scanning, including the risk of it being abused, before passing laws mandating its installation on millions of phones."

More information: Report: imperialcollegelondon.app.box. … pkc8etrkjwbo7mixki26

Conference: sp2023.ieee-security.org/

Provided by Imperial College London