Client-Side Scanning – UK Case

What It Is and Why It Threatens Trustworthy, Private Communication

December 2023

Summary and Recommendations

In the current scrutiny of the Online Safety Bill by the House of Lords, some debates have focused on end-to-end encryption (E2EE) and the use of "client-side scanning" technologies. The Internet Society seeks to contribute to this debate for three reasons: first, client-side scanning undermines the trust promised by end-to-end encryption, putting individuals' security and privacy at risk in the UK and beyond; second, the debate still includes misleading arguments which have persisted through earlier stages of the Bill and are not a reliable basis on which to assess the legislation; third, client-side scanning will not prevent motivated individuals from sharing illegal material without detection.

Recommendations

The Internet Society respectfully submits the following recommendations to Peers scrutinizing the Bill:

1. Support the amendment calling for private messaging services to be excluded from the scope of the Bill. [Amendments 203 and 204]
2. Remedy shortfalls in the safeguards provided in the Bill by supporting, for example, amendments that call for:
    a. An explicit prohibition of general monitoring, including the use of client-side scanning [Amendment 285]
    b. A requirement for technology notices to require judicial approval [Amendments 207 and 246]
    c. A requirement for Ofcom's interventions to be subject to a transparent and accountable public interest test [Amendment 208]
    d. An explicit duty for Ofcom to comply with human rights law [Amendment 214]
    e. An explicit duty for Ofcom to protect the privacy of the individual. [Amendments 209 and 210]

Regarding 2(a), the Online Safety Bill should rule out the mass *deployment* of technology that makes general monitoring possible, even if its stated intent is that such technology should only be *enabled* selectively. Such deployment would still represent a systemic weakness in mass market technology, and therefore a significant threat to cybersecurity and privacy.

Client-Side Scanning Violates Confidentiality

The Government continues to claim that Bill's duties to detect and prevent illegal material "do not ban or weaken encryption". This is misleading, *whether* such detection is based on a so-called encryption backdoor.[1] If, as the Government seems to envisage, detection is based on "client-side scanning", such scanning happens before the encryption process begins. While this may make the Government's claim pedantically true, confidentiality is lost as a result. The reality is that scanning nullifies the purpose of encryption, creates new security risks, and deprives citizens of the means to communicate in confidence.

Even the UK's national security professionals consider this proposal unsafe:

> "Client-side-scanning, despite the claims of its proponents, does seem to involve some kind of level of access, some kind of ability to sort and scan, and therefore there's no way of confining that to good use by lawful credible authorities and liberal democracies."
> — Ciaran Martin, former chief executive of the UK National Cyber Security Centre

It is legitimate to question the reliability of the claimed safeguards in the Bill, and to ask why the Government has thus far ignored the advice of informed national security professionals.

What Are the Risks of Client-Side Scanning?

Client-side scanning (CSS) broadly refers to systems, embedded on a user's phone or other device, that scan message contents (e.g., text, images, files) for matches or similarities to a database of objectionable content before the message is sent.

The more our lives and economies depend on online services and digital communication, the more vital it is for individuals, families, businesses, and governments to communicate securely, and with trust that their conversations and transactions are confidential. Providers of online communication services have increasingly implemented E2EE for their users, to improve security, privacy, and trust even when communication, inevitably, passes through one or more intermediaries. At the same time, governments

[1] "A Backdoor is a Backdoor is a Backdoor." Internet Society, 24 March 2020, https://www.internetsociety.org/blog/2020/03/a-backdoor-is-a-backdoor-is-a-backdoor/

and law enforcement agencies continue to seek access to communications, to detect and prevent crime.

Advocates of CSS technologies position them as the solution. However:

If breaking encryption is like steaming a letter open as it passes through a sorting office, client-side scanning is like reading the letter as it is being written. The result is the same: the privacy of the individual's communication is dead.

As a recent Joint Opinion[2] from the European Data Protection Board/European Data Protection Supervisor explains, CSS "can be easily circumvented by encrypting the content with the help of a separate application". CSS thus opens the door to disproportionate measures, which put citizens at risk and will not solve the problem of detecting illegal material from even slightly determined criminals.

Conclusion

Confidential communication is essential to a digital society and a data-driven economy, and E2EE is essential to confidential communication. Client-side scanning defeats the purpose of E2EE, fundamentally breaching the confidentiality that users expect and need when communicating online. What's more, CSS must be ubiquitous and pervasive to be effective, creating a vicious circle that the Online Safety Bill cannot square: if CSS is easily bypassed, it is pointless; if it is ubiquitous, it is disproportionate.

We already know that the Government wants all major communications platforms to be subject to this requirement. It is disingenuous for the Government to claim, at the same time, that this does not amount to a general monitoring obligation.

Client-side scanning, in mass-market consumer products and services:

- **Reduces confidence in the Internet ecosystem.** Loss of trust in online communication will damage the UK's economy at a time of extreme fragility.
- **Presents a serious risk to fundamental rights,** as expressed in the EDPB-EDPS Joint Opinion.
- **Imposes flawed security on users, including those most at risk,** with little prospect of preventing the actions of criminals or hostile governments.

[2] "EDPB-EDPS Joint Opinion 04/2022 on the Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse" 28 July 2022, https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-042022-proposal_en

The powers in the Online Safety Bill embody an obligation to detect illegal content in private communications. This is disproportionate, and its effectiveness is in doubt. The Government should strike this obligation from the Bill and focus instead on other, more effective ways of stopping networked crime and keeping users safe.

For More Information

Proponents of client-side scanning point to this technology as a solution for identifying objectionable content in E2EE environments. In this document, we have set out some of how CSS violates the trust agreement of E2EE and the dangers it presents.

For additional information about how CSS works, and its inherent flaws, the Internet Society's Fact Sheet on Client-Side Scanning can serve as a resource for detailed policy discussions.[3] Our other resources[4] about encryption, security, and privacy may also be useful for policymakers who are concerned but are not familiar with the topic.

About the Internet Society

The Internet Society is a global charitable organization founded in 1992 by some of the Internet's early pioneers. We believe the Internet is a force for good, and we are working towards an open, globally connected, secure, and trustworthy Internet that benefits everyone. With 110 active chapters across six continents, of which 28 are in Europe, and more than 100,000 individual users supporting our activities, the Internet Society is a significant stakeholder and a reliable, technically informed civil society interlocutor for Internet governance issues.

[3] "Fact Sheet: Client-Side Scanning." Internet Society, 26 Sept. 2022, https://www.internetsociety.org/resources/doc/2020/fact-sheet-client-side-scanning/

[4] "What Is Encryption?" Internet Society, 14 July 2022, https://www.internetsociety.org/issues/encryption/what-is/