Client-Side Scanning – EU Case

What It Is and Why It Threatens Trustworthy, Private Communication

December 2023

Abstract and Recommendations

The European Parliament has been reviewing the "proposal for a regulation laying down the rules to prevent and combat child sexual abuse" (CSA proposal). Some of the discussions have focused on end-to-end encryption as well as the use of "client-side scanning" technologies. The Internet Society seeks to contribute to this debate as the use of client-side scanning would undermine the trust assumptions promised by end-to-end encryption, putting the security and privacy of European Internet users at risk.

Recommendations

The Internet Society makes the following recommendations based on the European Commission's proposal:

1. That the European Committee introduce safeguards for end-to-end encryption.
2. That the European Committee prohibits the use of scanning technologies for general monitoring, including client-side scanning.

Client-Side Scanning Undermines the Trust Agreement of End-to-End Encryption

A common misconception is that you can have strong end-to-end encryption (E2EE) while simultaneously employing client-side scanning. This erroneous line of argumentation is based on the technicality that scanning happens *before* the encryption process begins. While this is true from a formal perspective, the reality is that scanning nullifies the purpose of encryption, creates new security risks, and puts the privacy of Europeans at risk.

If we all agree that encryption is a technology that protects us, we need to realize that client-side scanning invalidates its purpose.

What is Client-Side Scanning?

Client-side scanning (CSS) broadly refers to systems that scan message contents—i.e., text, images, videos, files—for matches or similarities to a database of objectionable content before the message is sent to the intended recipient.

What Are the Risks of Client-Side Scanning?

Major platform providers have increasingly implemented E2EE for their users to improve security, privacy, and trust. Simultaneously, law enforcement agencies increasingly seek access to message content to prevent the sharing of objectional content.

Companies that offer CSS technologies are positioning themselves as a solution. They claim to offer a technology that does not break or otherwise compromise encryption. However,

> Breaking encryption is like tampering with an envelope while it transits through a post office. Client-side scanning is like reading the letter as it is being written. In client-side scanning, the envelope is not tampered with, but the result is the same–the confidentiality agreement is violated.

Furthermore, as the EDPB-EDPS Joint Opinion[1] explains, CSS "can be easily circumvented by encrypting the content with the help of a separate application". This means that these techniques open the door to a disproportionate measure, putting every citizen at risk, without providing any real solution to the problem.

E2EE is an essential tool to ensure secure and confidential communications. CSS defeats the purpose of E2EE and fundamentally breaches the confidentiality that users expect when using E2EE communications tools. This breach in trust:

[1] "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

- **Presents a serious risk to fundamental rights,** as expressed in the EDPB-EDPS Joint Opinion.
- **Reduces trust in the Internet ecosystem.** Loss of trust is harmful to a digital economy and could derail EU ambitions for the Digital Decade.
- **Undermines security of communications and online services**, as identified by the Irish Parliament Joint Committee on Justice.[2]

Conclusion

Proponents of client-side scanning point to this technology as a solution for identifying objectional content in E2EE environments. However, this document has explained 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 information[4] about what is encryption and how it contributes to security and privacy may also be a valuable resource.

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.

[2] "Political Contribution on Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL laying down rules to prevent and combat child sexual abuse", Houses of the Oireachtas, Joint Committee on Justice, March 2023, https://opac.oireachtas.ie/Data/Library3/Documents%20Laid/2023/pdf/MTQzZG9jc2xhaWQzMDAzMjAyM18gMzAwMzIzXzEyMjEzMA==.pdf

[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/