



The EU Commission's New Proposal Would Undermine Encryption And Scan Our Messages

Description

The executive body of the European Union published today a legislative [proposal \(text\)](#) that, if it became law, would be a disaster for online privacy in the EU and throughout the world. In the name of fighting crimes against children, the EU Commission has suggested new rules that would compel a broad range of internet services, including hosting and messaging services, to search for, and report, child abuse material.

The Commission's new demands would require regular plain-text access to users' private messages, from email to texting to social media. Private companies would be tasked not just with finding and stopping distribution of known child abuse images, but could also be required to take action to prevent "grooming," or suspected future child abuse. This would be a massive new surveillance system, because it would require the infrastructure for detailed analysis of user messages.

The new proposal is overbroad, not proportionate, and hurts everyone's privacy and safety. By damaging encryption, it could actually make the problem of child safety worse, not better, for some minors. Abused minors, as much as anyone, need private channels to report what is happening to them. The scanning requirements are subject to safeguards, but they aren't strong enough to prevent the privacy-intrusive actions that platforms will be required to undertake.

Unfortunately, this new attempt to mandate a backdoor into encrypted communications is part of a global pattern. In 2018, the Five Eyes—an alliance of the intelligence services of Canada, New Zealand, Australia, the United Kingdom, and the United States—[warned](#) that they will "pursue technological, enforcement, legislative or other measures to achieve lawful access solutions" if the companies didn't voluntarily provide access to encrypted messages. With the [urging](#) of the Department of Justice, U.S. Congress tried to create backdoors to encryption through the EARN IT Act, in 2020 and [again earlier this year](#). Last fall, government agencies pressured Apple to propose a system of software scanners on every device, constantly checking for child abuse images and reporting back to authorities. Fortunately, the Apple [program appears to have been shelved for now](#), and EARN IT is still not law in the U.S.

The European Union prides itself on high standards for data protection and privacy, as demonstrated by the adoption of the General Data Protection Regulation, or GDPR. This new proposal suggests the EU may head in a dramatically different direction, giving up on privacy and instead seeking state-controlled scanning of all messages.

European civil society groups that deal with digital freedoms, including [European Digital Rights \(EDRi\)](#), Germany's [Society for Civil Rights](#), the Netherlands' [Bits of Freedom](#), and Austria's [epicenter.works](#) have expressed grave concerns about this proposal as well.

Fortunately, the misguided proposal published today is far from the final word on this matter. The European Commission cannot make law on its own. We don't think the EU wants to cancel everyday people's privacy and security, and we are ready to work together with Members of the European Parliament and EU member states' representatives to defend privacy and encryption.

By Joe Mullin

Category

1. Freedom-Free speech-Resistance & H-rights
2. Main
3. Politics-Geopolitics-Gov.-Events

Date Created

05/13/2022