Signal

October 3, 2025

For a future with privacy, not mass surveillance, Germany must stand firmly against client-side scanning in the Chat Control proposal

We are alarmed by reports that Germany is on the verge of a catastrophic about-face, reversing its longstanding and principled opposition to the EU's Chat Control proposal.

In a very real way it could spell the end of the right to privacy in Europe. Germany has long been a champion for privacy; drawing on its own history of the terrible harm that can be facilitated by mass surveillance and standing firm to safeguard this right for all of Europe. To capitulate now, at a time of great geopolitical uncertainty where the cybersecurity of our core infrastructures matters more than ever, would be an incomprehensible strategic blunder, and a fundamental betrayal of Europe's commitment to learn from history.

Under the guise of protecting children, the latest Chat Control proposals would require mass scanning of every message, photo, and video on a person's device, assessing these via a government-mandated database or AI model to determine whether they are permissible content or not.

This is a horrifying idea for many reasons. First, the technical consensus is clear. Scanning every message–whether you do it before, or after these messages are encrypted–negates the very premise of end-to-end encryption. Instead of having to break the gold-standard Signal encryption protocol to access someone's Signal messages, hackers and hostile nation states only need to piggyback on the access granted to the scanning system. This threat is so severe that even intelligence agencies agree it would be catastrophic for national security. These proposals ignore the strategic importance of private communications, and the longstanding technical consensus that you cannot create a backdoor that only lets the "good guys" in. What they propose is in effect a mass surveillance free-for-all, opening up everyone's intimate and confidential communications, whether government officials, military, investigative journalists, or activists. For all of Europe's talk of sovereignty, this is a bizarre cybersecurity decision on multiple fronts.

For Signal, Chat Control is also an existential threat. We do one thing and we do it very very well: we provide the world's largest truly private communications platform. And we know that encryption either works for everyone, or it doesn't work for anyone; a backdoor in one part of a network is a vector into every other part. And we will not compromise the integrity of our service, or endanger the safety of the people who rely on us around the world, often in contexts where private communications are the difference between life and death. If we were given a choice between building a surveillance machine into Signal or leaving the market, we would leave the market. This is not a choice we would make lightly, and our great hope is we never have to face it. But if Chat Control were enforced against us, that's likely where we would end up.

The good news is there is still time to stop this. The German government, particularly the Ministry of Justice, must hold the line. Good decision-making in Germany could spell the difference between a future where the human right to private communication exists in Europe or one in which Europe's economic, social, and political security are imperiled by Chat Control's mass surveillance free-for-all. We urge Germany to be wise and to stand firm in its principles. We cannot let history repeat itself, this time with bigger databases and much much more sensitive data.

Meredith Whittaker

President, Signal Foundation