Signal

June 17, 2024

New Branding, Same Scanning: “Upload Moderation” Undermines End-to-End Encryption

A statement from Meredith Whittaker, Signal President, in the context of the EU debate

End-to-end encryption is *the* technology we have to enable privacy in an age of unprecedented state and corporate surveillance. And the dangerous desire to undermine it never seems to die. For decades, experts have been clear: there is no way to both preserve the integrity of end-to-end encryption and expose encrypted contents to surveillance. But proposals to do just this emerge repeatedly — old wine endlessly repackaged in new bottles, aided by expensive consultancies that care more about marketing than the very serious stakes of these issues. These embarrassing branding exercises do not, of course, sway the expert community. But too often they work to convince non-experts that the risks of the previous plan to undermine end-to-end encryption are not present in the shiny new proposal. This is certainly how the EU chat control debate has proceeded.

In November, the EU Parliament lit a beacon for global tech policy when it voted to exclude end-to-end encryption from mass surveillance orders in the chat control legislation. This move responded to longstanding expert consensus, and a global coalition of hundreds of preeminent computer security experts who patiently weighed in to explain the serious dangers of the approaches on the table — approaches that aimed to subject everyone’s private communications to mass scanning against a government-curated database or AI model of “acceptable” speech and content.

There is no way to implement such proposals in the context of end-to-end encrypted communications without fundamentally undermining encryption and creating a dangerous vulnerability in core infrastructure that would have global implications well beyond Europe.

Instead of accepting this fundamental mathematical reality, some European countries continue to play rhetorical games. They’ve come back to the table with the same idea under a new label. Instead of using the previous term “client-side scanning,” they’ve rebranded and are now calling it “upload moderation.” Some are claiming that “upload moderation” does not undermine encryption because it happens before your message or video is encrypted. This is untrue.

Rhetorical games are cute in marketing or tabloid reporting, but they are dangerous and naive when applied to such a serious topic with such high stakes. **So let’s be very clear, again: mandating mass scanning of private communications fundamentally undermines encryption. Full stop. Whether this happens via tampering with, for instance, an encryption algorithm’s random number generation, or by implementing a key escrow system, or by forcing communications to pass through a surveillance system before they’re encrypted.** We can call it a backdoor, a front door, or “upload moderation.” But whatever we call it, each one of these approaches creates a vulnerability that can be exploited by hackers and hostile nation states, removing the protection of unbreakable math and putting in its place a high-value vulnerability.

We ask that those playing these word games please stop and recognize what the expert community has repeatedly made clear. Either end-to-end encryption protects everyone, and enshrines security and privacy, or it’s broken for everyone. And breaking end-to-end encryption, particularly at such a geopolitically volatile time, is a disastrous proposition.