European Commission wants to eliminate online confidentiality

DOSSIER: FREEDOM OF COMMUNICATION

11 mei 2022

FIGHTING CHILD SEXUAL ABUSE

This might sound attention-seeking, but we really believe to be not far off the mark. It really looks like the European Commission wants to cancel encryption.

Credits:
PHOTO: ASHLEY SMITH

Rejo Zenger
Beleidsadviseur

Do the impossible

Of course, that's not literally what the proposal says. The European Commission's proposal, which was launched today, will force companies to monitor what people share with each other via chat-apps like WhatsApp and platforms like Instagram. If deemed necessary, platforms will be forced to delete information or report it to the authorities. Internet service providers can also be ordered to monitor their customers' internet traffic. But the Commission omits, quite cleverly, depending on where you're standing, just how they should do so. Effectively her message for companies is: "Do the impossible, you get to decide how."

The proposal was launched today and can be found on the Commission's website

> **It is technically simply impossible to filter someone's internet connection the way the European Commission wants.**

Government mandated spyware

To give an example: based on this proposal an instant messaging platform can be given the task to detect material of the sexual exploitation of children. That could be known material, or "new" material, or grooming, so text. Let's assume, for the sake of the argument, that the order is given to Meta with regards to Whatsapp. A platform that, as you know, is protected with end-to-end encryption. This type of encryption means Meta can see who is communicating with whom, but is unable to read the content of that communication. But how is Meta supposed to detect something in a conversation it's not supposed to be able to access? For the sake of convenience, the Commission leaves that decision (the "how to do it") to the platform. Our guess is that the only way to do it, is by installing some sort of (now, government mandated!) spyware on the phones of the people using a particular service. After all, that is the only place where the content of the chats is readable.

What can go wrong, will go wrong

And yes, there are a few safeguards built into the proposal. For example, an order can only be given if "reasonable risk mitigation measures" haven proven to be insufficient. And only if the reasons for issuing the order "outweigh the adverse consequences for the rights and legitimate interests of all concerned". Based on that, you could argue that installing spyware on every person's phone would never be a proportionate measure if your interest is detecting and removing particular bits of information from particular devices. But the proposal also says "the choice of technology is up to the company, as long as the requirements of this law are met." Years of experience unfortunately leads us to interpreting proposed legislation from the most pessimistic of viewpoints. What can go wrong, will sooner or later go wrong.

> **We are gearing up for an intensely emotional political debate.**

Technically impossible

Even if you would be so inclined, there is little reason for optimism. For example, the proposal will allow authorities to have access to certain URLs blocked. These could be specific pages, such as 'https://www.bitsoffreedom.nl/doneren', or specific images on that page. Nowadays, almost all websites are only accessible through a secure TLS connection (the "s" in "https://"). So is ours. When you visit the web page you're currently on, the connection between your browser and the server where the website is "stored", is encrypted. Because of that encryption, your provider can only tell you are visiting our website, but not which page or its contents. Your provider cannot see the full URL. And that means it is technically impossible to filter your internet as the European Commission would like providers to do. That is - unless we simply abolish encryption or expect providers to manipulate your internet traffic.

An intensely emotional political debate

We need to brace ourselves for an intensely emotional political debate. The proposed measures would severely undermine the confidentiality of our communications, and are being presented in the context of an incredibly sensitive and important topic, which is the protection of children from sexual abuse. This is going to be a debate in which rational arguments, even more so than usual, are going to have a tough run of it.

If confidential communication is dear to you, please donate!

Already disastrous

Regardless of the exact outcome, the proposal has already been harmful because it discourages companies from making their services more secure by developing and deploying encryption. After all, against the backdrop of this proposal any such step could be interpreted as purposefully placing children in a more vulnerable position. As a decision to hinder the fight against the sexual abuse of children. No company will want to go there. If a company was planning on implementing end-to-end encryption for an existing service, those plans have now undoubtedly been put on hold. And with that, even if the European Commission's proposal were ultimately to be shot down, it has already done its damage.

Indispensable for everyone

Oh, and it goes without saying that everyone, including us, considers the fight against the sexual abuse of children to be extremely important. That's precisely why it's crucial to focus on effective and sustainable measures. This proposal does not meet those standards. The confidentiality of communication is indispensable for everyone, including for children and victims of sexual abuse. You can only communicate safely with a trusted friend, counselor, social worker or law enforcement officer if you can be sure no one is looking over your shoulder. The European legislator should therefore focus on other measures. For example, streamlining cross-border criminal investigations, strengthening cooperation between different services and eliminating the huge backlog of cases within the police's vice squad.

Europese Commissie wil vertrouwelijkheid op internet opheffen