It's official. Your private communications can (and will) be spied on

On 6 July, the European Parliament adopted in a final vote the derogation to the main piece of EU legislation protecting privacy, the ePrivacy Directive, to allow Big Tech to scan your emails, messages and other online communications.

What is all of this about?

If you are in shock and need first some background reading, we recommend you to read more about where all of this comes from. Read our previous blogposts **here** and **here**. In essence, the adopted interim Regulation (it is a temporary Regulation that will cease to be valid in December 2022) allows the *continuation* of *voluntary* scanning of all communications all the time by certain service providers to detect and report to authorities online child sexual abuse material (CSAM). The final text is available **here**.

Why should I be worried?

As a whole, the legislation is a negative evolution in the sense that it will legalise the continuous *voluntary* scanning of all communications by private companies. The services under the scope of the interim Regulation are as broadly defined as in the ePrivacy Directive, including your Facebook Messenger messages, Tinder chats, emails and any other form of online communication that will come up in the future is potentially under the scope.

Continuing? Is Big Tech already reading my private communications?

We understand this is surprising but yes, with the initial proposal it became clear that an undefined number of platforms/services were already scanning unencrypted private communications. When the Commission was asked what was the legal basis for such practices, they **admitted they had no clue**. In essence, if you're not using end-to-end encrypted communications you must assume that the company running the service will be scanning your communications.

Voluntary scanning of my messages? Who's up to do that?

Good question! There is no official list of services and applications, but it looks like Facebook at least is already doing this, and others may follow. Yes, **your Tinder spicy conversations may be scanned too**.

Why now?

First, there is a legal reason. Because the **European Electronic Communications Code (EECC)** entered into force, most online communication services are obliged to respect privacy and confidentiality. As we **explained elsewhere** already, this should have been good news, but the proponents of weak privacy and confidentiality of communications argued that enforcing these new rules would lead to the European Union becoming a "**safe haven for peadophiles**".

The second reason is that Facebook decided to encrypt Facebook Messenger conversations with end-to-end encryption (as it is the case on their other product WhatsApp). The encryption of these conversations would prevent Facebook (and anyone else) from reading the content of your conversations, which allegedly would reduce the number of CSAM detected by these platforms. Consequently, they claim that this would result in decreasing the number of suspects being taken to court (and more illegal material being disseminated).

How long will this madness last? Can I do something?

The interim Regulation will be in force until December 2022, and in the meantime the long-term legislative solution will be developed and adopted. The long-term CSAM legislation is expected to be proposed by the Commission in October 2021. There is nothing we can do as regards the interim Regulation. However, we recommend you to contact **our local digital rights organisations** and ask how you can help ahead of the upcoming long-term legislation that will substitute the one that just got adopted.

What does the interim Regulation look like?

In a nutshell, the worst aspect of this interim Regulation is that it creates a dangerous **precedent** to allow companies or governments to read your private communications and online interactions, for example to prevent terrorism or for "national security" reasons. It also feeds the general, recurring narrative that **encryption** protects criminals (**in this tweet** from the European

Commission the point on encryption is illustrated by a person wearing a balaclava). According to **lead Members of the European Parliament**, the discussions were rushed and put under immense pressure. They went further in saying that the legislation would not even resist a serious analysis if it was challenged before the Court of Justice of the European Union (CJEU).

What is bad about it?

– The legislation will allow the continuation of ***voluntary*** scanning of ***all*** **communications** ***all*** **the time** by certain service providers, instead of promoting a targeted approach that focuses on genuine suspects for a limited period of time.

– A specific practice called **grooming** (sexual solicitation of children) is part of the scope, which means that not only known illegal images but also the content of your messages will be scanned, which is more intrusive. This would need to be authorised by Data Protection Authorities (DPAs) and companies would need to carry out a Data Protection Impact Assessment (DPIA) before deploying their technologies.

– As we mentioned above, the scope of services and platforms under the scope remains quite broad and unspecific. And it **could equally cover** social media private chats (e.g. Instagram and Facebook), dating apps and videoconferencing tools.

What gives us a bit of hope?

– The interim Regulation protects (in recitals) **end-to-end encryption**. This may not be the case in the upcoming CSAM long-term legislation, so be ready for **Cryptowars 3.0**.

– The technologies used to achieve the goals of the Regulation need to be the **least privacy-invasive,** state-of-the-art and can only be used for the strict purpose of detecting and reporting CSAM, not for any other purposes.

– **DPIAs** are mandated for **current and future** technologies, and DPAs are the supervisory authorities to ensure scanning practices are in line with data protection requirements

– the **European Data Protection Board (EDPB)** will ensure the oversight of the scanning practices and technologies used, and has to prepare guidelines on which technologies could be used. This safeguard, in theory, could halt practices which are not necessary and proportionate.

– There are **reporting** obligations (Article 3g on "Statistics") including the number of convictions following the use of these technologies, the number of false positives, the differentiation between the absolute number of cases and cases reported multiple times, and the type of provider of online communications services where the online child sexual abuse was detected. This will bring some clarity on the efficiency of these practices (which helps to clarify the "necessity" part in the necessity and proportionality test).

Autumn is coming: Get ready for the long-term legislation

Do not get fooled by the positive improvements that the European Parliament was able to insert in the text. The Regulation sets a bad precedent for private communications and it is likely to get worse with the long-term legislation that will be proposed in Autumn 2021, meant to substitute this interim legislation. Rumours say that encrypted communications will fall in the scope, and that this time an **obligation** will be put on private companies to stalk our communications, not just a legalisation of what was already happening (and which was very likely illegal).

Human rights organisations need to engage with child protection associations and explain how it will affect children's rights, how little it will help them (as **some abuse survivors said themselves**). This is probably one of the most crucial digital dossiers right now, and we will need as many of you as possible if we want to protect freedom of expression, privacy and confidentiality of children and everyone else.

The article was published on 7 July 2021.

Diego Naranjo

Head of Policy

Twitter: **@DNBSevilla**

Defending your rights online

European Digital Rights (EDRi) is an association of civil and human rights organisations from across Europe. We defend your rights and freedoms in the digital environment.

Quick links

Contact us

About us

Media relations

Take action

Together, we can build a people-centered, democratic society!

Stay up to date via the EDRi-gram

Attend an event

Follow us

Twitter

Facebook

LinkedIn

YouTube

Privacy policy

Website by Reason Digital