European Politicians Declare War On Text Message Privacy

The same EU politicians who are trying to censor the Internet now want to read all of your personal messages and break encryption



CECÍLIE JÍLKOVÁ AND ALEX GUTENTAG

APR 30, 2024 PAID



EU Commissioner for Home Affairs Ylva Johansson (right) on March 4, 2024 in Brussels, Belgium. (Photo by Thierry Monasse/Getty Images)

In recent weeks, Public has documented how ruling European politicians appear to have weaponized government intelligence agencies to

discredit and censor their political enemies.

Now, Public has learned that the European Union is close to winning new legislation that would allow it to monitor *all* private digital conversations, from text messaging to emails. The new law would give EU police the power to read all messages on Gmail, WhatsApp, and other mail and text messaging services.

The politicians, who are Members of the European Parliament (MEPs), say their legislation will be limited to "individuals or groups… linked to child sexual abuse using "reasonable grounds of suspicion.'" And, they said, "To avoid mass surveillance or generalised monitoring of the internet, the draft law would allow judicial authorities to authorise time-limited orders…"

But the technology companies themselves such as Apple say such "automatic data scanning" is technically impossible without compromising privacy and security. The new law would require Facebook, X, YouTube, Telegram, Snapchat, TikTok, and cloud services and online gaming websites to constantly monitor and report any evidence of child sexual abuse material (CSAM) on their systems and in the private chats of their users. And messaging apps including Signal, Proton Mail and Tutanota would no longer have end-to-end encryption.

As a result, "Millions of private conversations and private photos of law-abiding citizens are about to be searched and leaked using flawed technology without even a remote connection to child sexual abuse," warned Patrick Breyer, a privacy activist and former member of the European Parliament who opposes the proposed modifications to the law, known as "Chat Control."

The details of the new law leaked on April 2 and were published in the subscribers' section of the French news site contexte.com. The draft contains the full text of the regulation, which people close to the process say means that it is getting readied for approval.

All of this is very shocking. There is no evidence of any increase in child exploitation that merits this panic. Europeans have historically cared more about privacy than Americans, and have put in place strong privacy protections for their citizens. Why is it now seeking such a massive invasion of privacy? Why is the EU on the verge of enacting mass surveillance?

“Chat Control” As Information Control



Patrick Breyer (Pirate Party), plaintiff in the hearing on whether the federal government may save the IP addresses of all visitors to its websites at the Federal Supreme Court (BGH), answers journalists' questions ahead of trial in Karlsruhe, Germany, 14 February 2017. Photo: Uli Deck/dpa | usage worldwide (Photo by Uli Deck/picture alliance via Getty Images)

The EU’s “Chat Control” is not the first attempt to undermine encryption. WhatsApp and Telegram have been in the censorship

industry's crosshairs since late 2018, when free speech on texting apps was blamed for allowing then-candidate Jair Bolsonaro to become president of Brazil.

In March 2021, Rob Flaherty, the Biden White House's director of digital strategy, demanded that Meta, the owner of messenger app WhatsApp, moderate private conversations on its platform.

Large philanthropies have promoted spying on text messages for several years "There is currently no easy way to discover potentially problematic content on WhatsApp and other end-to-end encrypted platforms at scale," lamented censorship advocates in a January 2022 Omidyar Foundation report.

"One potential solution is to make use of misinformation 'tiplines' to identify potentially misleading or otherwise problematic content," the report concluded. "On WhatsApp, a tipline would be a phone number to which WhatsApp users can forward potential misinformation they see to have it fact-checked."

EU institutions have been discussing mandatory control of private messages for almost two years. The EU Commissioner for Home Affairs, Ylva Johansson, and several NGOs, the most prominent of which are Thornand ECPAT, are all behind the current proposed legislation.

The proposed law is excessively "influenced by companies that pretend to be NGOs but behave more like technology companies", Arda Gerkens, former director of Europe's oldest online CSAM reporting hotline, told Balkan Insight last September.

"Groups like Thorn are using everything they can to bring forward this legislation, not only because they feel it is the way forward in the fight against child sexual abuse, but also because they have a commercial interest in it," Arda Gerkens added.

Meredith Whittaker, president of the American non-profit Signal Foundation, the company behind the encrypted chat app Signal, said at the European Digital Rights (EDRi) conference on September 26, 2023, "we're in the midst of a storm of global attacks on the human right to privacy with governments Security Services, AI companies masquerading as NGOs and a lot of money with very little transparency hard at work trying to walk back the few safe havens we've been able to carve out against the ferocious surveillance business model and the states that skim off of it."

In an interview with Balkan Insight, Whittaker said that AI companies that produce scanning systems are effectively establishing themselves as clearing houses and liability buffers for large technology companies and feel the market potential. "The more they frame this as a huge problem in the public discourse and in front of regulators, the more they incentivize big tech companies to trust them to solve problems," Whittaker said.

According to Whittaker, these AI firms are essentially offering tech companies a "free pass from liability" by telling them, "'Pay us [...] and we will [...] maintain the AI system, we will do whatever it takes to magically clean up the problem.'"

According to EDRi, it is possible that providers will rely on "already existing infrastructure, such as the PhotoDNA software" to comply with "Chat Control." This technology is linked to efforts to prevent "extremism."

PhotoDNA was created in 2009 by Microsoft Research in cooperation with Dartmouth College professor Hany Farid. Farid has also emerged as one of the world's leading authorities on the spread of online disinformation— and how to bring it under control.

PhotoDNA creates a unique signature for a digital image, which can be compared with the signatures of other images to find copies of that

image. According to EDRi, use of PhotoDNA tool would mean that, “In the event of the file being identified as relevant, this would not only allow to block the message from being forwarded but also an alert to be given to the police as well.”

Farid and PhotoDNA did not respond to Public’s request for comment.

The European Commission's December 2023 report refers to PhotoDNA as “the most widely used tool [...] used by over 150 organizations. PhotoDNA has been in use for more than 10 years and has a high level of accuracy.“

Microsoft already uses its PhotoDNA — in combination with artificial intelligence — in a number of its products, including Skype, OneDrive and Xbox. Microsoft donated PhotoDNA to the National Center for Missing & Exploited Children (NCMEC).

As of 2022, PhotoDNA was widely used by online service providers including Google's Gmail, Twitter,Facebook, Adobe Systems, Reddit, Discord to help find, report and eliminate some of the images of child pornography online.

In June 2016, Farid, then working as a senior advisor to the Counter Extremism Project (CEP), unveiled a software tool for use by Internet and social media companies to quickly find and eliminate extremist content used to spread and incite violence and attacks. It functions similarly to PhotoDNA.

To operationalize this new technology to combat extremism, Farid and CEP proposed the creation of a National Office for Reporting Extremism (NORex), which would house a comprehensive database of extremist content and function similar to the National Center for Missing & Exploited Children.

In December 2016, Facebook, Twitter, Google and Microsoft announced plans to use PhotoDNA to tackle extremist content such as terrorist recruitment videos or violent terrorist imagery. However, according to EDRi, "the definition of "extremist content" is everything but clear; CEP's algorithm does not (and logically cannot) contain this definition either."

Farid also specializes in the analysis of digital images and the detection of digitally manipulated images such as deepfakes. A deepfake detector designed by Farid and Czech student Matyáš Boháček to identify unique facial expressions and hand gestures can spot manipulated videos.

"We need government oversight," professor Farid said in an interview about disinformation in November 2023. "Europeans are doing a good job of it. They came out with a dossier recently, the Digital Safety Act. The Brits are coming out with an online safety bill. The Australians have passed one. The Americans? The Americans are lost at sea."

PhotoDNA can recognize not only images but also videos. It can therefore identify all copies of deepfake videos on the Internet. Or videos that contain child pornography. Or videos that incite extremism. Or videos that contain disinformation or hate speech. It only depends on the assignment.

Germany And Encryption Activists Fight Back



Messaging app Signal's President Meredith Whittaker at the Web Summit, Europe's largest tech event, in Lisbon on November 14, 2023. (Photo by PATRICIA DE MELO MOREIRA/AFP via Getty Images)

The EU politicians, pro-censorship philanthropies, and the NGOs they fund all appear dead set on waging war on privacy. They want to finalize their proposal by June 9, when the European Parliament elections are due to take place. A European Commission spokesperson told Public, "the Commission continues to support the co-legislators to ensure that negotiations [on the proposed regulation] can be concluded as soon as possible."

The European Parliament's official timetable schedules the adoption of a position on compulsory chat control by EU interior ministers for 13-14 June 2024. The actual adoption of the regulation is then scheduled for after the elections. "The risk that it can go [to approval] quickly is high," one insider warned Public, "especially now that MPs like Patrick Breyer are no longer in Parliament."

But growing resistance means there is still time for privacy advocates to derail the legislation. Today, European and German data protection authorities, over 100 international digital and civil rights organizations, and end-to-end encrypted service providers like Signal, led by outspoken encryption advocate, Whittaker, are fighting “Chat Control.”

Some whole governments are opposed. Representatives of the German government, which is far more concerned about privacy than censorship, sent 61 questions to the Commission challenging the shortcomings of the proposed legislation. In its letter, it specifically asked how the draft law is compatible with certain provisions of the General Data Protection Regulation (GDPR) or how the law can guarantee that technology will not be misused. In its statement to the European Commission, the German government asks that the bill be brought into line with "constitutional standards for the protection of private and confidential communications."

The government also called for compliance with the Charter of Fundamental Rights of the European Union: "Confidentiality of communication is an important value to protect in our liberal societies,” wrote the Germans. “Based on the Charter of Fundamental Rights, everyone has the right to respect for their private and family life, home and communication. Any regulatory measures must be proportionate, should not go beyond what is necessary to prevent child sexual abuse in the digital space, and must effectively balance the competing interests of protecting children from abuse on the one hand and protecting privacy on the other."

In a letter to the Commission, the Senate of the Kingdom of the Netherlands recalled that the draft law had been widely criticized by national data protection authorities, including the European Data Protection Board(EDPB), and said that the members of the Dutch parliamentary parties also considered that this criticism should be taken very seriously.

The German Child Protection Association and representatives of the investigating authorities have rejected the random checking of private files and communications as disproportionate. The world's leading IT security researchers and a number of scientists have also voiced their criticism.

Fans in German football stadiums are protesting against this new form of mass surveillance. Two thirds of all young people in Europe reject chat control.

Lawyers have also criticized the legislation: The German Bar Association warns of a "massive infringement of civil liberties", while the Irish Parliament's Legal Affairs Committee has sent a letter to the European Commission in which it does not support the draft regulation.

The Legal Service of the Council of the EU has also criticized the project from a legal point of view and considers the inspection of private chats to be illegal.

A study by the EU Parliament's Scientific Service also strongly criticizes the plans - and even the EU Commission's own evaluation warns against the plans.

The current Belgian presidency of the European Council has responded to all these concerns by claiming to have put forward a "more proportionate" proposal that protects encryption. However, this was not borne out in the latest version of the proposal published by contexte.com.

The latest proposal from the Belgian Council Presidency has once again met with opposition from civil society: 48 organizations from across Europe have issued an open letter calling for a rejection of this “lazy compromise.” In their open letter, these organizations and individuals state, “Despite some nominal changes to the risk categorization

framework, the new proposal still allows for the use of discovery orders on a broad basis and without targeting."

According to EDRi, commissioner Johansson has "become some of the most urgent and one-sided voices lobbying for a law that will treat everyone as a suspect and will enforce mass surveillance of almost our entire digital lives." EDRi has conducted an investigation into Johansson's claims about the CSA Regulation and – based on solid evidence – has assessed that Johansson is repeatedly serving inaccurate and misleading claims about how technology works, what the law could really achieve in practice, and what current detecting practices have shown.

"If EU governments actually enter the trilogue negotiations with this radical position, experience shows that Parliament risks gradually abandoning its original position behind closed doors and making bad and dangerous compromises that fundamentally jeopardise our online security," Breyer warns.