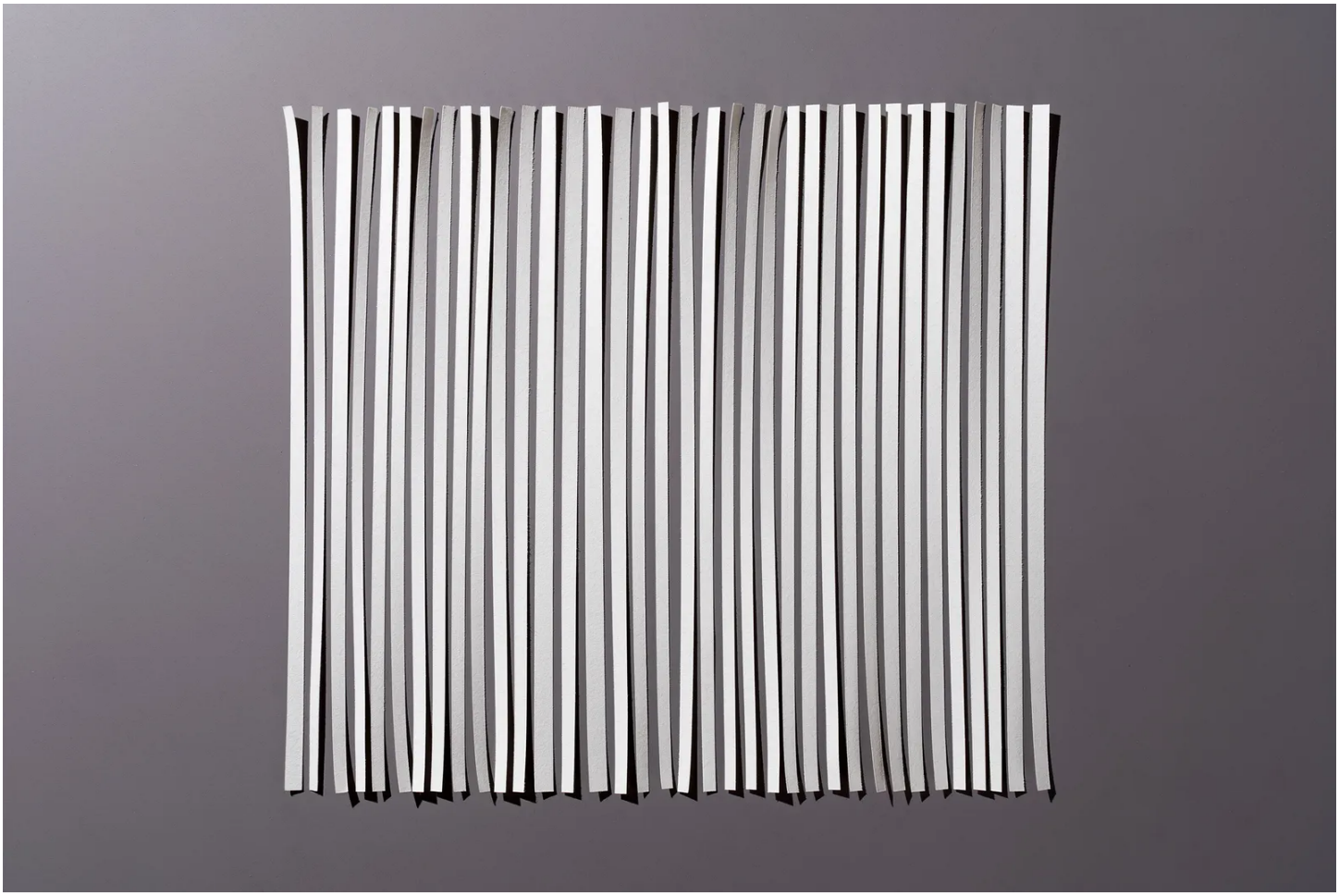
LILY HAY NEWMAN MORGAN MEAKER MATT BURGESS SECURITY MAY 22, 2023 3:23 PM

Leaked Government Document Shows Spain Wants to Ban End-to-End Encryption

In response to an EU proposal to scan private messages for illegal material, the country's officials said it is “imperative that we have access to the data.”



PHOTOGRAPH: MIRAGEC/GETTY IMAGES

SPAIN HAS ADVOCATED banning encryption for hundreds of millions of people within the European Union, according to a leaked document obtained by WIRED

that reveals strong support among EU member states for proposals to scan private messages for illegal content.

The document, a European Council survey of member countries' views on encryption regulation, offered officials' behind-the-scenes opinions on how to craft a highly controversial law to stop the spread of child sexual abuse material (CSAM) in Europe. The proposed law would require tech companies to scan their platforms, including users' private messages, to find illegal material. However, the proposal from Ylva Johansson, the EU commissioner in charge of home affairs, has drawn ire from cryptographers, technologists, and privacy advocates for its potential impact on end-to-end encryption.

For years, EU states have debated whether end-to-end encrypted communication platforms, such as WhatsApp and Signal, should be protected as a way for Europeans to exercise a fundamental right to privacy—or weakened to keep criminals from being able to communicate outside the reach of law enforcement. Experts who reviewed the document at WIRED's request say it provides important insight into which EU countries plan to support a proposal that threatens to reshape encryption and the future of online privacy.

Of the 20 EU countries represented in the document leaked to WIRED, the majority said they are in favor of some form of scanning of encrypted messages, with Spain's position emerging as the most extreme. "Ideally, in our view, it would be desirable to legislatively prevent EU-based service providers from implementing end-to-end encryption," Spanish representatives said in the document.

The source of the document declined to comment and requested anonymity because they were not authorized to share it.

"It is shocking to me to see Spain state outright that there should be legislation prohibiting EU-based service providers from implementing end-to-end encryption," says Riana Pfefferkorn, a research scholar at Stanford University's Internet Observatory in California who reviewed the document at WIRED's request. "This document has many of the hallmarks of the eternal debate over encryption."

End-to-end encryption is designed so only the sender and receiver of communications like messages can see their contents. This boxes out all other

parties, from scammers to police and even the company providing the digital platform. Law enforcement advocates often propose creating technical mechanisms through which end-to-end encryption can be bypassed for investigations, but cryptographers and other technologists have long argued that this would introduce weaknesses that inherently undermine end-to-end encryption, putting users' privacy at risk. Furthermore, they have repeatedly concluded that this expanded exposure would ultimately hurt the digital safety and security of vulnerable groups, including children, rather than defend them.

"Breaking end-to-end encryption for everyone would not only be disproportionate, it would be ineffective of achieving the goal to protect children," says Iverna McGowan, the secretary general of the European branch of the Centre for Democracy and Technology, a digital rights nonprofit organization, who reviewed the document at WIRED's request.

The leaked document contains the position of members of the police Law Enforcement Working Party, a group of the Council of the European Union that deals with law enforcement views on legislation. Dated April 12, 2023, the document contains 20 countries' views on a series of questions, including whether they see end-to-end encryption as a hindrance to their work dealing with child sexual abuse and whether they would favor adding wording to the law to stipulate that encryption shouldn't be weakened. The questions were first posed in January.

WIRED asked all 20 member states whose views are included in the document for comment. None denied its veracity, and Estonia confirmed that its position was compiled by experts working within related fields and at various ministries.

The document reveals strong support for Johansson's proposal to scan private end-to-end encrypted communications for illegal content. Of the 20 countries included in the document, 15 expressed support for the idea of scanning end-to-end encrypted communications for CSAM. Many framed this type of scanning as a vital tool that would enable authorities to win the fight against child abuse.

"It is of utmost importance to provide clear wording in the CSA Regulation that end-to-end encryption is not a reason not to report CSA material," Croatia's representatives said in the document. "Detection orders must necessarily also

apply to encrypted networks," Slovenia said. "We don't want E2EE encryption to become a 'safe haven' for malicious actors," Romania added.

Denmark and Ireland expressed support for scanning encrypted messengers for child sexual abuse material while also endorsing the inclusion of wording in the law that protects end-to-end encryption from being weakened. The ability to do this would rely on the invention of technology that can scan encrypted messages for illegal content without altering or breaking the security features offered by encryption—a feat cryptographers and cybersecurity experts have said is technically impossible.

The Netherlands, however, stated that this would be possible through "on-device" scanning before the illegal material is encrypted and sent to its recipient. "There are … technologies which may allow for automatic detection of CSAM while at the same time leaving end-to-end encryption intact," the country's representatives stated in the document.

"They want to keep the security of encryption whilst being able to circumvent it," says Ella Jakubowska, a senior policy advisor at European Digital Rights (EDRI). Jakubowska says she is "unsurprised but nevertheless shocked" to see that European countries have a "really shallow understanding" of encryption. "They want privacy but they also want to indiscriminately scan encrypted communications," Jakubowska says.

In its response, Spain said it is "imperative that we have access to the data" and suggests that it should be possible for encrypted communications to be decrypted. Spain's interior minister, Fernando Grande-Marlaska, has been

outspoken about what he considers the threat posted by encryption. When reached for comment about the leaked document, a spokesperson for Spain's Ministry of Interior said the country's position on this matter is widely known and has been publicly disseminated on several occasions. Edging close to Spain, Poland advocated in the leaked document for mechanisms through which encryption could be lifted by court order and for parents to have the power to decrypt children's communications.

Jakubowska, who reviewed the document, says that several countries appear to say they would give police access to people's encrypted messages and communications. Comments from Cyprus, for example, say it is "necessary" that law enforcement authorities have the ability to access encrypted communications to investigate online sexual abuse crimes and that the "impact of this regulation is significant because it will set a precedent for other sectors in the future." Similarly, officials in Hungary say "new methods of data interception and access are needed" to help law enforcement.

"Cyprus, Hungary, and Spain very clearly see this law as their opportunity to get inside encryption to undermine encrypted communications, and that to me is huge," Jakubowska says. "They are seeing this law as going far beyond what DG home is claiming that it's there for."

Officials in Belgium said in the document that they believe in the motto "security through encryption and despite encryption." When approached by WIRED, a spokesperson from Belgium's Ministry of Foreign Affairs initially shared a statement from the country's federal police saying its position has evolved since it submitted comments for the document and that Belgium is adopting a position, alongside other "like-minded states," that it wants encryption weakened. However, half an hour later, the spokesperson attempted to retract the statement, saying the country declined to comment.

Security experts have long said that any potential backdoors into encrypted communications or ways to decrypt services would undermine the overall security of the encryption. If law enforcement officials have a way to decipher messages, criminal hackers or those working on behalf of governments could exploit the same capabilities.

Despite the potential attack on encryption from some countries, many nations also appeared to strongly support end-to-end encryption and the protections it

provides. Italy described the proposal for a new system as disproportionate. “It would represent a generalized control on all the encrypted correspondence sent through the web,” the country’s representatives said. Estonia cautioned that if the EU mandates the scanning of end-to-end encrypted messages, companies are likely to either redesign their systems so they can decrypt data or shut down in the EU. Triin Oppi, a spokesperson for Estonia’s Ministry of Foreign Affairs, says the country’s position had not changed.

Finland urged the EU Commission to provide more information about the technologies that can fight child sexual abuse without jeopardizing online security and warned that the proposal could conflict with the Finnish constitution.

Representatives from Germany—a country that has staunchly opposed the proposal—said the draft law needs to explicitly state that no technologies will be used that disrupt, circumvent, or modify encryption. “This means that the draft text must be revised before Germany can accept it,” the country said. Member states need to agree on the text for the draft bill before the negotiations can move forward.

“The responses from countries such as Finland, Estonia, and Germany demonstrate a more comprehensive understanding of the stakes in the CSA regulation discussions,” Stanford’s Pfefferkorn says. “The regulation will not only affect criminal investigations for a specific set of offenses; it affects governments’ own data security, national security, and the privacy and data protection rights of their citizens, as well as innovation and economic development.”
Read the full document below: