INTERNATIONAL ENCRYPTION BRIEF

MARCH 2021

The Encryption Debate in the European Union: 2021 Update

Maria Koomen

Carnegie Endowment for International Peace
Publications Department
1779 Massachusetts Avenue NW
Washington, DC 20036
P: + 1 202 483 7600
F: + 1 202 483 1840
CarnegieEndowment.org

This publication can be downloaded at no cost at CarnegieEndowment.org.

About the Encryption Working Group

The Carnegie Endowment for International Peace and Princeton University have convened a small group of experts to advance a more constructive dialogue on encryption policy. The working group consists of former government officials, business representatives, privacy and civil rights advocates, law enforcement experts, and computer scientists. Observers from U.S. federal government agencies attended a select number of working group sessions. Since 2018, the working group has met to discuss a number of important issues related to encryption policy, including how the relevant technologies and uses of encryption will evolve in the future.

This brief and its companion pieces detailing the encryption debates in a select number of key countries and regions—Australia, Brazil, China, the European Union, Germany, and India—were prepared by local and area experts at the request of the Encryption Working Group. They are designed to shine light on key drivers of the debates in these countries, how they have evolved in the last five years, and the divergent approaches taken by different governments. The briefs do not take a position on encryption policy, rather they provide analysis of how debates about encryption have evolved internationally. The views are the authors' own and do not necessarily reflect the views of Carnegie or the Encryption Working Group.

Introduction

The encryption debate in the European Union (EU) continues to evolve, with new drivers, stronger tools, and increasingly higher stakes. The debate among policymakers and experts is maturing, but there is a widening knowledge gap between political elites and the public around encryption. In Europe, encryption is perceived in two conflicting ways. It is a tool for privacy and security and therefore is an essential component of Europe's open societies and markets; but it is also argued to be a shroud for criminal activity and therefore an obstacle to law enforcement. Efforts to weaken or break encryption to combat crime also undermines European privacy and security.

Europe's recent encryption debate was sparked in 2016 by a string of terror attacks that exposed flaws in Europe's collective ability to counter terrorism. In the wake of these attacks, Europol and national law enforcement authorities pointed to encryption as a key threat and serious impediment to the detection, investigation, and prosecution of such criminal activity.[1] With this, member states demanded a European policy solution to encryption,[2] igniting the current EU-wide encryption debate.[3]

In 2017, the EU responded with a series of provisional, non-legislative measures to study the issue and expand training and resources for law enforcement. The measures focused on data "at rest"—data stored on encrypted devices—but also included informal discussions on end-to-end encryption with experts from law enforcement and the judiciary, academia, nongovernmental organizations (NGOs), over-the-top service providers, telecommunication providers, and the security industry.[4]

Since then, an increase in reported child sexual abuse online has fueled and conflated the EU encryption debate, further driving political support for legislation to get around encryption. With this new driver, the current EU debate departs from previous iterations in the sophistication of its technical proposals, which go beyond previous law enforcement calls for mere "backdoors" and may set a dangerous precedent for other global debates to include technical solutions.

The European Commission, which began its current leadership term in 2019, has embarked on an ambitious set of priorities,[5] including to create a "Europe fit for the digital age." Its priorities focus on strengthening the right to privacy and connectivity, improving the free flow of data, and bolstering cybersecurity in Europe—all of which are built upon strong encryption. So how can the EU balance political calls for legislation to break encryption with its priority to protect strong encryption?

Encryption and Child Sexual Abuse Material

Reports of online child sexual abuse have dramatically increased in the last decade. According to the U.S. National Center for Missing and Exploited Children, global reports of child abuse have risen from 23,000 in 2010 to over 725,000 in 2019.[6] The EU has become the largest geographical hub of child sexual abuse material (CSAM) globally, with almost nine in ten reported URLs hosted in Europe.[7]

Of those reported, over 94 percent of cases were on Facebook and its platforms—Messenger, Instagram, and WhatsApp—using content filtration technology.[8] In the same year, Facebook announced its vision for a "privacy-focused" social network, including deployment of end-to-end encryption (E2EE) across its services.[9] This would effectively render 70 percent of the CSAM cases on Facebook undetectable to both law enforcement and Facebook itself.

Facebook's announcement alarmed law enforcement and child protection organizations, whose response entrenched online child abuse as a key driver in Europe's encryption debate. In response, European Commissioner for Home Affairs Ylva Johansson called for a "technical solution" to the "problem" of encryption.[10] This language is reminiscent of that used by EU member states around encryption as an obstacle to antiterrorism in 2016,[11] which effectively sparked the current encryption debate.

Reports of online child abuse, and the subsequent calls for lawful access to encrypted data for investigation, have continued to increase during the coronavirus pandemic as government-enforced lockdowns left children at home with minimal supervision.[12] According to Europol's 2020 "Internet Organised Crime Threat Assessment,"[13] there was a sharp spike in reported CSAM, often on peer-to-peer networks like Facebook Messenger, although the report does not provide evidence to explain this spike. With more offenders isolated at home, the crisis also increased demand for CSAM by as much as 25 percent in some EU member states.[14] Tragically, so long as the pandemic persists, offenders producing CSAM for a profit are expected to increase supply to meet the growing demand.[15]

Security Through and Despite Encryption

In response, in July 2020, the European Commission launched two important strategies—one for combating child sexual abuse specifically, and another for updating the EU's Security Union Strategy more broadly—which both pointed to encryption from a public safety and security standpoint as means for perpetrators to "mask their identity" and "hide their actions from law enforcement."[16] Specifically, the Strategy to Combat Child Sexual Abuse laid out a comprehensive plan including

sector-specific regulations, operational efforts, and technical solutions, which highlight the role of the private sector and call on companies "to detect and report child sexual abuse in E2EE communications." The updated EU Security Union Strategy confirmed that the EU will "explore and support balanced technical, operational and legal solutions" to these so-called challenges imposed by encryption and "promote an approach which both maintains the effectiveness of encryption in protecting privacy and security of communications, while providing an effective response to crime and terrorism."

Later that summer, a leaked draft discussion paper revealed details behind the European Commission's thinking about technical "solutions" to detect CSAM in E2EE communications. The analysis of technical solutions presented in the draft was more technically nuanced than past rhetoric in EU encryption debates because it focused on the client side, or technology provider side, and the detection of CSAM. Unsurprisingly, however, the draft did not identify a silver bullet solution. Instead, as Mallory Knodel, chief technology officer at the Center for Democracy and Technology, pointed out, the draft made available a "least bad" option, which could be a persuasive, albeit manipulative, tactic. In fact, a new Global Encryption Coalition of privacy and free expression advocates argued that, although the discussion paper suggested some solutions may be less risky than others, each would put the privacy, safety, and security of billions of users worldwide at risk, ultimately "making everyone – including the children we are trying to protect – more vulnerable to the crimes we collectively are trying to prevent."[17]

Meanwhile, an unintended legislative knot—the combination of gridlock over updates to privacy legislation, dubbed the ePrivacy Directive, and the sunset of the European Electronic Communications Code—created legal ambiguity about whether it was lawful for technology platforms in the EU to filter electronic communications services for the detection of CSAM. Alarmed by the potential new challenge of scale in combating online child abuse, the European Commission proposed a so-called e-privacy derogation from the safeguards of the ePrivacy Directive to make it mandatory for companies to (continue to) filter content, encrypted or not, for CSAM. Negotiations among EU lawmakers stalled in December, with the European Parliament arguing that the proposal did not live up to EU privacy rules. While regulators all over the world—democratic and undemocratic—are pushing for technology-based solutions to encryption, this debate showcases the complexity and conflicting interests involved.

Despite these conflicting interests, the German presidency of the Council of the European Union pressed ahead with a proposed council declaration on encryption. The proposal called for the creation of a "balance" between "security through encryption and despite encryption."[18] The proposal called on EU member states to "join forces with the tech industry" to jointly create this balance, and to define and establish a regulatory framework as well as innovative approaches and best practice to respond to these challenges.

Testing the Balance

Such political calls for exceptional access to encrypted content by EU member state justice ministers and international counterparts are being met with calls for stronger encryption "to become the norm," from other government and institutional entities, as well as from civil society, academia, and industry.[19] But can the EU really create such a balance to provide security through and despite encryption?

Legally, no. Existing EU-wide legislation identifies encryption as a possible measure to ensure an appropriate level of security for the protection of fundamental rights and data, and to strengthen cybersecurity.[20] Considering the scale of the CSAM problem in Europe, though, the case could be made for an EU-level exception to either regulate against the use of encryption in certain circumstances or to warrant government access to encrypted data in the name of CSAM investigation and prosecution. However, as outlined in the May 2019 brief,[21] even if EU legislation were to be passed, data access policies and capabilities differ among member states so problems with encryption in criminal investigations vary from one member state to another.[22] This variation across member states, coupled with qualms of insufficient mutual legal assistance treaties (MLATs), was the problem that initially pushed the encryption debate to the EU level. In this framework, EU legislation would be ineffective as it would rely on existing member state capabilities—or lack thereof—for enforcement.

Technically, no, not without effectively breaking or undermining encryption. As the European Commission outlined in its working document, there is no single technological solution to provide law enforcement access to encrypted data and rather several different solutions with varying degrees of effectiveness, feasibility, privacy, security, and transparency. However, these recommended solutions de facto break end-to-end encryption as they pre-filter messages before they are encrypted and sent.[23] As digital rights watchdog Diego Naranjo argues, this undermines the crucial technological safeguard of encryption.[24] Finally, even if the EU decided to adopt one of these technical models, it would have to rely on private industry actors for implementation.

In addition to legal and technical complexities, there are several risks of scanning and filtering encrypted communication for illegal content. For example, considering the universal condemnation of child abuse, CSAM may be the most feasible entry point to discuss encrypted communications. But in the context of combating terrorism and other harmful content, it is far more complex due to legal ambiguities of such content and the violations any scanning system could impose on users'

fundamental freedoms. Such technology would need to be paired with a robust legal framework with safeguards and accountability measures, or it would be up to industry alone to choose which technology to use in what circumstances—a choice that may come down to cost and feasibility to deploy. On the other hand, such technology could also be deployed to filter and target speech for the suppression of political dissidents, journalists, or human rights defenders.

Beyond filtration technologies, there's a range of cryptographic functionalities being developed for communication services that hand privacy and security controls over to platforms, third parties, or even users. One expert, Seny Kamara at Brown University, noted that companies are making it possible for users to verify or deny, or even anonymize different types of encryption settings when using communications services.[25] This means that, if a user receives illegal content, they could unencrypt the conversation for reporting to law enforcement. However, even if these features became available to users, European governments and institutions would need to create clear, secure, and reliable paths for users to report such content to law enforcement, as well as awareness and redress mechanisms for those being reported.

Considering there are arguably no legal or technical recipes for such a balance between security through and despite encryption, the EU must create a political solution to its political question. Despite this and the legal complexities and technical risks involved the EU's calling on tech companies to create that balance confirms that a political solution isn't enough. As one critical observer tweeted, it is a "clever political solution" by the commission to "solve the impossible problem of law enforcement agencies' access without mandating encryption backdoors: put companies in charge of weakening the security of their own communication services!"[26] Further, any political solution would undermine previous calls for safeguarding communication that helps keep Europe's online society and economy running.[27]

Outlook

On encryption in general, the European Council adopted a resolution on encryption in November 2020, signaling EU member states' readiness to join forces with industry, create said balance between security despite and through encryption, design a regulatory framework, and innovate investigative capabilities around encryption.[28]

In the meantime, the European Commission folded discussions about CSAM and encryption into the annual EU Internet Forum ministerial meeting on terrorism. In this year's ministerial, which convened EU member states, online platforms, Europol, and academia, the commission presented the outcomes of its expert consultation process—the final version of its leaked working paper—and in response, participants recognized the "need to find technology solutions" to challenges "created by technology."[29] Further, Home Affairs Commissioner Ylva Johansson urged council and parliament negotiators to come to an agreement on the e-Privacy Derogation, and revealed that the commission is working on "permanent legislation" on CSAM that makes it obligatory for tech companies to report and remove child sexual abuse, encrypted or not.[30]

Boldly, the European Parliament Intergroup on Children's Rights warned that, without this legislation, the EU would become a "safe haven for pedophiles."[31] Diego Naranjo pointed out similar claims mixing encryption and scanning of private communications with riots and child abuse in the *Guardian*,[32] the *New York Times*,[33] and *Fortune*,[34] warning that "posing scanning of private communications as a dilemma between child protection and privacy is a false dichotomy," as children and activists, too, require privacy.[35]

With the continuation of such high-level political support for technical solutions, Europe's encryption debate is further entrenched in debates around child sexual abuse and terrorism—or, more broadly, criminality.

Looking forward, the European Commission is expected to communicate its ambition and strategy for achieving such solutions in spring 2021. What shape and direction they will take remains to be seen, but one can look to the commission's working document for a hint. The resolution is a step toward needed legal reform and a constructive—albeit vague—start to necessary risk assessment and public consultation for a more nuanced debate around encryption in Europe.

However, despite the EU signaling readiness to proceed with a regulatory framework on encryption, and the EU's progress on forthcoming legislation to fight against CSAM online, much is still at stake for fundamental rights, rule of law, and democratic principles in the European debate around encryption.

European and international civil society organizations and industry players have coalesced around the topics and brought the European encryption debate from behind closed doors into the public domain. The European Digital Rights (EDRi) association addressed a series of open letters from civil society to the EU highlighting five fundamental rights problems of these pursuits as: (1) lacking

clarity of services covered and the legal basis for current practices; (2) lacking impact assessment and key public consultations; (3) risking the normalization of exceptional measures; (4) empowering big tech companies, putting private companies in charge of surveillance and censorship mechanisms that, because of their impact on fundamental rights, should be the responsibility of public authorities; and (5) potentially attacking encryption.[36]

In a recent letter to the president of the European Commission, EDRi and signatories called for open consultation and public dialogue on the proposal to legislate encryption in the fight against CSAM. It also called on the European data protection supervisor and the Fundamental Rights Agency to work together with the EU institutions, civil society, and industry to find democratic solutions and acceptable legal framework for shared problems.[37]

Beyond these open letters and calls to action for stronger encryption, privacy and human rights advocates caution against using politically charged issues like terrorism and child abuse to justify weakening encryption for law enforcement because such rhetoric narrows the debate and fuels misunderstanding about encryption's larger role in the prevention and investigation of crime. These fundamental rights advocates are joined by wider civil society and some industry actors to argue against legislation that mandates law enforcement access to encrypted data because the benefit of strong widespread encryption to the public outweighs the relatively small obstacle it poses to law enforcement. The Center for Democracy and Technology, Global Partners Digital, and the Internet Society, plus more than thirty other civil society organizations have formed the above-mentioned Global Encryption Coalition to pool research and advocacy efforts toward stronger encryption worldwide. In the private sector, a tech alliance of small and medium-sized enterprises has formed under the name Encryption Europe, with a joint position for stronger encryption, "zero backdoors," and transparency with regard to encryption algorithms.[38]

Looking ahead, considering the complexity of the debates around encryption and the essential role it plays in Europe's open societies and markets, it is important that the EU takes next steps in close cooperation not only with industry but also with civil society in order to ensure public access to, deliberation on, and understanding of the issues and their implications as well as accountability.

About the Author

Maria Koomen leads the Open Governance Network for Europe, a joint initiative of the Open Government Partnership and Democratic Society.

Notes

1 "The Internet Organised Crime Threat Assessment," Europol, September 28, 2016, https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2016.

2 "German-French Letter Concerning Cooperation Between Law Enforcement Agencies and Electronic Communication Service Providers," Council of the European Union, November 7, 2016, http://data.consilium.europa.eu/doc/document/ST-14001-2016-INIT/en/pdf.

3 Catherine Stupp, "Give Member States Want EU-Wide Laws on Encryption," Euractiv, November 22, 2016, https://www.euractiv.com/section/social-europe-jobs/news/five-member-states-want-eu-wide-laws-on-encryption.

4 Maria Koomen, "The Encryption Debate in the European Union," Carnegie Endowment for International Peace, May 30, 2019, https://carnegieendowment.org/2019/05/30/encryption-debate-in-european-union-pub-79220.

5 "2021 Commission Work Programme – From Strategy to Delivery," press release, European Commission, October 19, 2020, https://ec.europa.eu/commission/presscorner/detail/en/ip_20_1940.

6 National Center for Missing and Exploited Children, website, accessed March 13, 2021: https://www.missingkids.org/gethelpnow/cybertipline.

7 "IWF 2019 Annual Report | Zero Tolerance," Internet Watch Foundation, April 27, 2020, https://www.iwf.org.uk/what-we-do/who-we-are/annual-reports.

8 "2019 Reports by Electronic Service Providers (ESP)," National Center for Missing and Exploited Children, 2019, https://www.missingkids.org/content/dam/missingkids/gethelp/2019-reports-by-esp.pdf.

9 Mark Zuckerberg, "A Privacy-Focused Vision for Social Networking," Facebook, 2019, https://www.facebook.com/notes/mark-zuckerberg/a-privacy-focused-vision-for-social-networking/10156700570096634/.

10 Ylva Yohansson, "Speech by Commissioner Johansson at Webinar on 'Preventing and Combating Child Sexual Abuse and Exploitation: Towards an EU Response'," European Commission, June 9, 2020, https://ec.europa.eu/commission/commissioners/2019-2024/johansson/announcements/speech-commissioner-johansson-webinar-preventing-and-combating-child-sexual-abuse-exploitation_en.

11 Lucie Krahulcova, "EU Ministers Are Targeting Encryption. We Need to Know More.," Access Now, November 8, 2016, https://www.accessnow.org/eu-ministers-targeting-encryption-need-know.

12 Alasdair Sandford, "Coronavirus: Half of Humanity Now on Lockdown as 90 Countries Call for Confinement," Euronews, April 2, 2020, https://www.euronews.com/2020/04/02/coronavirus-in-europe-spain-s-death-toll-hits-10-000-after-record-950-new-deaths-in-24-hou.

13 "Exploiting Isolation: Offenders and Victims of Online Child Sexual Abuse During the COVID-19 Pandemic," Europol, June 19, 2020, https://www.europol.europa.eu/publications-documents/exploiting-isolation-offenders-and-victims-of-online-child-sexual-abuse-during-covid-19-pandemic; and Europol, "Internet Organised Crime Threat Assessment," October 5, 2020, https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2020.

14 Ibid.

15 Ibid.

16 "Communication from the Commission on the EU Security Union Strategy," European Commission, July 24, 2020, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52020DC0605&-from=EN; and "Communication from the Commission on the EU Strategy for a More Effective Fight Against Child Sexual Abuse," European Commission, July 24, 2020, https://ec.europa.eu/home-affairs/

sites/homeaffairs/files/what-we-do/policies/european-agenda-security/20200724_com-2020-607-commission-communication_en.pdf.

17 "Breaking Encryption Myths," Global Encryption Coalition, November 19, 2020, https://www.globalencryption.org/2020/11/breaking-encryption-myths/.

18 "Draft Council Declaration on Encryption – Security Through Encryption and Security Despite Encryption," Council of the European Union, October 21, 2020, https://data.consilium.europa.eu/doc/document/ST-12143-2020-INIT/en/pdf.

19 Statewatch, "Germany Asks What Should the EU Do About Encryption for Law Enforcement?," European Digital Rights (EDRi), October 14, 2020, https://edri.org/our-work/germany-asks-what-should-the-eu-do-about-encryption-for-law-enforcement/.

20 Article 32(1a), 34(3a), 6(4e), recital (83) of Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC; recital (60), article 31(3a) of the Law Enforcement Directive; recital (20) in conjunction with article 4 of the ePrivacy Directive 2002/58/EC; recital (40) of Regulation (EU) 2019/881 (Cybersecurity Act).

21 Koomen, "The Encryption Debate in the European Union."

22 Europol and Eurojust, "Second Report of the Observatory Function on Encryption," Europol, February 18, 2020, https://www.europol.europa.eu/publications-documents/second-report-of-observatory-function-encryption

23 Patrick Beuth, "Verschlüsselung bitte nur für gute Menschen," Spiegel Netzwelt, September 8, 2020, https://www.spiegel.de/netzwelt/netzpolitik/eu-kommission-gegen-kindesmissbrauch-verschluesselung-bitte-nur-fuer-gute-menschen-a-8db88bf2-29c8-495c-83e9-818bf05d7d85.

24 Diego Naranjo, "Open Letter: Civil Society Views on Defending Privacy While Preventing Criminal Acts," European Digital Rights, October 27, 2020, https://edri.org/wp-content/uploads/2020/10/20201020-EDRi-Open-letter-CSAM-and-encryption-FINAL.pdf.

25 Seny Kamara, "Content Moderation in E2EE Systems: What Is Actually Possible?," online event, Center for Democracy and Technology, December 9, 2020, https://www.youtube.com/watch?v=khqdw6-9B7Q&ab_channel=CenterforDemocracy%26Technology.

26 Jesper Lund on Twitter, September 24, 2020, https://twitter.com/je5perl/status/1309099006505750529.

27 "Cybersecurity," European Commission, accessed March 16, 2021: https://ec.europa.eu/digital-single-market/en/cybersecurity.

28 "Council Resolution on Encryption – Security Through Encryption and Security Despite Encryption," Council of the European Union, November 24, 2020, https://data.consilium.europa.eu/doc/document/ST-13084-2020-REV-1/en/pdf.

29 "EU Internet Forum Ministerial : Towards a Coordinated Response to Curbing Terrorist and Child Sexual Abuse Content on the Internet," European Commission, January 26, 2021, https://ec.europa.eu/home-affairs/news/eu-internet-forum-ministerial-towards-coordinated-response-curbing-terrorist-and-child-sexual_en.

30 Commissioner Ylva Johansson, "Commissioner Johansson's speech at the EU Internet Forum Ministerial Meeting," European Commission, January 25, 2021, https://ec.europa.eu/commission/commissioners/2019-2024/johansson/announcements/commissioner-johanssons-speech-eu-internet-forum-ministerial-meeting_en.

31 Co-chairs of the Intergroup on Children's Rights, "We Cannot Risk That the EU Becomes a Safe Haven for Paedophiles," Vote for Children, January 22, 2021, https://www.childrightsmanifesto.eu/we-cannot-allow-the-eu-to-become-a-safe-haven-for-paedophiles-and-sexual-predators-online/.

32 Vikram Dodd, "Facebook's Encryption Plans Could Help Child Abusers Escape Justice, NCA Warns," *Guardian*, November 23, 2020, https://www.theguardian.com/uk-news/2020/nov/23/facebooks-encryption-plans-could-help-child-abusers-escape-justice-nca-warns.

33 Brian X. Chen and Kevin Roose, "Are Private Messaging Apps the Next Misinformation Hot Spot?," *New York Times*, February 3, 2021, https://www.nytimes.com/2021/02/03/technology/personaltech/telegram-signal-misinformation.html.

34 Jonathan Vanian, "Private Messaging Apps Signal and Telegram Are Red Hot After the Capitol Riots," *Fortune*, January 14, 2021, https://fortune.com/2021/01/13/messaging-apps-signal-telegram-capitol-riots/.

35 Diego Naranjo, "Wiretapping Children's Private Communications: Four Sets of Fundamental Rights Problems for Children (and Everyone Else)," European Digital Rights, February 10, 2021, https://edri.org/our-work/children-private-communications-csam-fundamental-rights-issues/.

36 Statewatch, "Germany Asks What Should the EU Do About Encryption for Law Enforcement?," European Digital Rights (EDRi), October 14, 2020, https://edri.org/our-work/germany-asks-what-should-the-eu-do-about-encryption-for-law-enforcement/.

37 Naranjo, "Open Letter."

38 "Position Paper : An Introduction to Encryption in Europe," Encryption Europe, January 2021, https://encryptioneurope.eu/positionpaper/.

CARNEGIE
ENDOWMENT FOR
INTERNATIONAL PEACE

1779 Massachusetts Avenue NW | Washington, DC 20036 | P: + 1 202 483 7600

CarnegieEndowment.org