INTERNATIONAL ENCRYPTION BRIEF

MAY 2019

The Encryption Debate in the European Union

Maria Koomen

The Encryption Debate in the European Union

Maria Koomen

For your convenience, this document contains hyperlinked source notes as indicated by teal colored text.

© 2019 Carnegie Endowment for International Peace. All rights reserved.

Carnegie does not take institutional positions on public policy issues; the views represented herein are the author's own and do not necessarily reflect the views of Carnegie, its staff, or its trustees.

No part of this publication may be reproduced or transmitted in any form or by any means without permission in writing from the Carnegie Endowment for International Peace. Please direct inquiries to:

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.

CONTENTS

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 briefing paper 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.

The Encryption Working Group will continue its efforts to study this important issue and plans on releasing further briefings on aspects of the encryption policy debate.

Members of the Encryption Working Group include:

Jim Baker
Former General Counsel, Federal Bureau of Investigation

Katherine Charlet
Program Director, Technology and International Affairs, Carnegie Endowment for International Peace

Tom Donahue
Visiting Fellow, George Mason National Security Institute, and former Senior Director for Cyber Operations, National Security Council, White House

Ed Felten
Robert E. Kahn Professor of Computer Science and Public Affairs, Princeton University

Avril Haines
Senior Research Scholar at Columbia University's Columbia World Projects and former Deputy Director, Central Intelligence Agency

Susan Hennessey
Executive Editor, Lawfare, and Senior Fellow in Governance Studies, the Brookings Institution

Chris Inglis
Managing Director, Paladin Capital Group, and former Deputy Director, National Security Agency

Sean Joyce
US Cybersecurity and Privacy Leader, PwC, and former Deputy Director, Federal Bureau of Investigation

Susan Landau
Bridge Professor of Cyber Security and Policy, Tufts University

Christy Lopez
Distinguished Visitor from Practice, Georgetown Law Center

Alex Macgillivray
Board Member, Data & Society, and former Deputy Chief Technology Officer of the United States

Jason Matheny
Founding Director, Georgetown Center for Security and Emerging Technology, and former Director, Intelligence Advanced Research Projects Activity

Tim Maurer
Co-Director and Fellow, Cyber Policy Initiative, Carnegie Endowment for International Peace

Denis McDonough
Visiting Senior Fellow, Technology and International Affairs, Carnegie Endowment for International Peace, and former White House Chief of Staff

Lisa Monaco
Distinguished Senior Fellow, Reiss Center on Law and Security, New York University School of Law, and former Assistant to the President for Homeland Security and Counterterrorism

Laura Moy
Executive Director, Center on Privacy & Technology, Georgetown Law Center

Michelle Richardson
Director, Privacy and Data Project, Center for Democracy and Technology

Ronald L. Rivest
Institute Professor, Massachusetts Institute of Technology

Ari Schwartz
Managing Director of Cybersecurity Services, Venable LLP

Harlan Yu
Executive Director, Upturn

Denise Zheng
Senior Associate (Non-resident), Technology Policy Program, Center for Strategic and International Studies

Note: This is not a comprehensive list of all members. Some wish to remain anonymous for the time being and to contribute in their personal capacity.

Since the 1990s, encryption has become an essential component of Europe's open societies and markets. The encryption market has burgeoned in Europe, and the technology has flourished, protecting everything from financial transactions to in-vehicle information, from confidential health data to private communications. But a string of terror attacks in Europe sparked a contentious European Union (EU) debate on encryption. As fears of terrorism intensified, EU member states called for stronger collective measures to prevent and counter it. Europol and national law enforcement authorities pointed to encryption as a key threat to the detection, investigation, and prosecution of such criminal activity in Europe. With this, member states demanded a European policy solution, igniting a contested policy debate around encryption in the European Union.

Introduction

The question of what role the EU should play in managing encryption-related issues within its borders is a contested one, and recent debates are tied up in zero-sum equations reminiscent of the first Crypto War in the 1990s. Were the EU to mandate that law enforcement be granted access to encrypted data and devices to help prevent terrorism and solve crimes, what would be the potential implications for the fundamental rights of its citizens and the integrity of its cross-border networks and markets? Conversely, how can the EU promote strong encryption in the name of privacy and security without enabling a safe haven for crooks and terrorists, thereby further impeding the role of intelligence and law enforcement authorities (LEAs) in preventing terror and solving crime?

As in other governments around the world, the EU is confronted with multiple perspectives on each encryption issue—but no viable policy solution is in sight. As such, the current European Commission will likely not legislate on encryption before the end of its term in October 2019, and it will be up to the next commission to reset any legislative mandate for the 2019–2024 term. Instead, the EU is focusing the remainder of its 2014–2019 term on provisional, nonlegislative measures, such as increasing investment in Europol, funding police trainings across member states, and consulting with different stakeholders. These moves would help the union gain a deeper understanding of the technical and legal aspects of the issues and explore options for possible future legislation on these issues.

Background

One of the problems that sparked and ostensibly fueled recent EU policy debates on encryption is terrorism. Several terror attacks hit Europe in 2014, with more following in 2015 and 2016. As fears of terrorism intensified, EU member states called for stronger collective measures to prevent and counter it. According to the 2016 Europol Internet Organized Crime Threat Assessment, member states' law enforcement authorities pointed to encryption as a key threat and serious impediment to the detection, investigation, and prosecution of such criminal activity. With this mantra, several

member states demanded a European policy solution, igniting a contested EU policy debate around encryption.

Although terrorism has been the main driver of recent debates around encryption at the EU level, there are other serious tensions shaping the discourse. Encryption has risen to become an essential component of Europe's open societies and markets. The European Commission's 2017 cybersecurity strategy recognized encryption as a vital tool for the protection of personal data and fundamental rights, such as privacy and the freedom of expression. Encryption has been hailed by the EU Fundamental Rights Agency as a means to reinforce security and privacy, cornerstones of EU policy, as it allows those who need it—from journalists to human rights defenders, banks to ordinary internet users—to shield their internet communications and safeguard personal data against unauthorized access or leaks.

However, encryption has become an increasing concern for LEAs related to cases of not only terrorism but also child sexual abuse, corruption, cyber crime, and other types of organized crime and trafficking in and beyond the EU. In this regard, LEAs point to encryption as an obstacle to criminal investigation, and therefore, a threat to security in Europe. Further, as data access policies and capabilities differ among member states, problems with encryption in criminal investigations vary from one member state to another. Legal frameworks for cooperation between member states and states outside the EU are slow and considered inadequate for addressing terrorism and other cross-border criminal cases involving encrypted information.

Key Actors

The main players in current EU debates around encryption are those pushing for or against a European policy solution. Those pushing for EU legislation are member states' law enforcement authorities. Germany, France, and the United Kingdom are among the loudest member states that have taken public positions on encryption, called for European legislation, and have passed or are preparing national legislation. It was these member states' concerns that opened debates in 2016 in the context of terrorism and criminal investigation and elevated those debates to the European level.

Actors publicly pushing against a European policy on encryption are academics, technologists, and civil society organizations like Access Now and European Digital Rights (EDRi). In response to initial discussions that began the current closed-door debates, these groups demanded information and public consultations, urged the Council of the EU to reject calls for policies that would prevent or undermine the use of strong encryption, called out the commission for struggling to find a position on encryption, and made much of these otherwise off-the-record debates available to the public.

Key industry associations, such as Business Europe and Digital Europe, have called for encryption to be encouraged to protect not only intellectual property but also the businesses they represent from "cyber-theft of critical technologies, trade secrets, and other confidential business information." After the commission announced its nonlegislative measures in 2017, tech companies continued to push for safeguards. A Digital Europe spokesperson warned, "any operational capabilities to decrypt data should be subject to independent oversight and enforcement."

In the European institutions, Andrus Ansip, the commission vice president for the Digital Single Market, has said he opposes laws that force companies to create backdoors to weaken encryption. Europol's European Cybercrime Centre (EC3) and Eurojust are working in an "observatory function" to assess the technical and legal aspects of encryption in the context of criminal investigations at the EU level, as well as areas of cooperation in need of improvement and reform. Europol, the EU's law enforcement agency, and ENISA, the EU's cybersecurity agency, signed an agreement in May 2016 opposing laws that oblige companies to provide backdoors to encrypted technologies and services. They agreed that "built-in backdoors to encryption don't provide a secure fix to police frustrations." The directors of the two agencies said that "while [backdoors] would give investigators lawful access in the event of serious crimes or terrorist threats, it would also increase the attack surface for malicious abuse, which, consequently, would have much wider implications for society."

This joint agreement was made despite contradictory statements about the "going dark" problem made by Europol in its 2016 Internet Organized Crime Threat Assessment and by Europol's chief, Rob Wainwright, who publicly denounced encryption as the "biggest problem for the police and the security service authorities in dealing with the threats from terrorism" only days prior to signing the agreement. This contradiction exemplifies the many political inconsistencies among EU institutions on encryption.

Beyond political discrepancies at the EU level, there has been considerable debate about the effectiveness of European legislation, should it ever be imposed, on encryption in general. Regarding criminal investigations, the EU has no enforcement mandate, so European legislation would depend on member state authorities. Some member states, however, do not have the financial or technical capacity to enforce such legislation. Further, as a 2016 EU Council questionnaire revealed, member states have different experiences with and capacities for solutions to encryption in criminal investigations. This variation across member states, coupled with qualms of insufficient mutual legal assistance treaties (MLATs), was the problem that initially pushed the recent policy debate to the EU level. So, in this framework, EU legislation would be arguably ineffective, as it would rely on existing member state capabilities—or lack thereof—for enforcement.

In the meantime, Europol, has been supporting member states in developing a set of decryption tools and methods to break encryption without backdoors, and has urged stronger LEA cooperation with industry partners and the crypto-analysis research community "for the breaking of encryption

where lawfully indicated." Europol and ENISA concluded in the aforementioned agreement that "a solution that strikes a sensible and workable balance between individual rights and protection of EU citizens' security interests can be found."

Main Issues

September 2016 EU Council Questionnaire

As fears of going spotty or even going dark in the fight against terrorism escalated, EU interior ministers met in July 2016 to discuss the "issue of encryption" with regard to access to communications data in criminal investigations. Shortly thereafter, France and Germany signed a joint letter to the European Commission calling for a European "solution to encryption." In the following series of closed-door conversations, the Council of the EU issued a questionnaire to interior ministers to assess concretely what issues LEAs faced around encryption and how they were responding.

Under mounting pressure from civil society and a freedom of information request submitted by Dutch internet rights group Bits of Freedom, the council declassified the questionnaire and leaked a summary of responses. It revealed, among many other insights, that while member state ministers generally agreed that encryption should be protected, EU countries struggle with encryption and security protocols to varying degrees.

- Problems expressed by member states pointed mainly to a lack of technical expertise and computer processing power in law enforcement, inadequate MLATs, and the absence of frameworks for public-private and cross-border coordination.
- The technologies that have spurred political concern are primarily unrecoverable full disk encryption software, such as TrueCrypt, VeraCrypt, and DiskCryptor, and the increasingly ubiquitous end-to-end encrypted online email and messaging applications. Specifically, member states have raised concern about virtual private networks (VPNs), Hypertext Transfer Protocol Secure (HTTPS), Secure Shell (SSH) tunneling, Pretty Good Privacy (PGP), Invisible Internet Project (I2P), and Tor, as well as electronic communication services like Signal, Skype, Telegram, and WhatsApp—all listed by member states' LEAs as tools increasingly used by suspects. Debates about these technologies revolve around the impact they have on the ownership of and access to personal data in devices, applications, and the internet. As Euractiv reported, seven EU countries responded that authorities come up against encrypted data during criminal investigations, and some LEAs "almost always" encounter encryption.
- Five countries said that they want the commission to provide legislation that would make it easier for LEAs to access encrypted information and share data with investigators in other countries.[1]

- Some countries wanted EU legislation to focus on access to data stored remotely on cloud services, which are often operated by companies based in other EU countries or outside the twenty-eight-member bloc. Polish officials wrote that "one of the most crucial aspects will be adopting new legislation that allows for acquisition of data stored in EU countries 'in the cloud,'" without forcing LEAs to request data through cumbersome official exchange agreements.
- Most countries responded that their police forces lack the funds and technical capability to intercept encrypted criminal communications, demanding EU help to bolster national means to crack encryption technology.
- Member states expressed more frustration over encryption impeding the gathering of evidence rather than access to data for surveillance.

With mounting pressure from member states on the one hand and increasing pushback from civil society, academia, and industry on the other, the Council of the EU published a report to frame a formal meeting on encryption issues around terrorism and security in December 2016. In that meeting, interior ministers agreed on a new European Commission mandate for the remainder of the 2014–2019 term to assess the concrete technical, legal, and political issues surrounding encryption in criminal investigations in order to identify solutions that strike a balance between individual rights and citizen security and privacy versus allowing law enforcement agencies to do their job.

With this new mandate, the European Commission started exploring the aspects and implications of encryption through private consultations with relevant stakeholders, drawing upon the expertise of European agencies such as Europol, Eurojust, ENISA, and Fundamental Rights Agency (FRA), as well as member states' law enforcement agencies, industries, academia, and civil society organizations.

October 2017 European Commission Position

After several months of private consultation, in October 2017, the commission announced its first position on the role of encryption in criminal investigations. This included a set of technical measures aiming to support member state authorities:

- support Europol to further develop its decryption capability;
- develop an expert network to support national law enforcement and judicial authorities;
- create a toolbox of alternative investigation techniques to obtain needed information encrypted by criminals;
- set up "better and more structured collaboration" between authorities, service providers, and other industry partners to promote a better mutual understanding of the existing and evolving challenges on all sides;

- provide 500,000 euros funding for national training programs for law enforcement and judicial authorities; and
- continue assessing technical and legal aspects of the role of encryption in criminal investigations, in collaboration with the EC3 at Europol and Eurojust.

This announced position was embedded in the commission's anti-terrorism package, which, in principle, framed encryption narrowly as a setback for law enforcement authorities. The report also stated that "the use of encryption is essential to ensure cybersecurity and the protection of personal data. EU legislation specifically notes the role of encryption in ensuring appropriate security for the processing of personal data." With this, the commission expressly omitted measures to prohibit, limit, or weaken encryption, thereby maintaining that encryption will not be regulated in the short term. However, observers like EDRi have noted that even the commission's nonlegislative approach has implications for stakeholders, as encryption workarounds highlight the shortcomings of current laws and policies and could worsen situations where they fail to protect fundamental rights. Others raised concerns that this approach fails to safeguard encryption in the longer term, leaving the door open to future legislation toward so-called backdoors for law enforcement to access private data.

Technical Measures

With this announcement, Julian King, the European commissioner in charge of security, emphasized that the EU was shifting away from earlier debates about possible legislation requiring companies to create backdoors for LEAs. Instead, the EU will move toward a more hands-on approach for developing member state techniques and capabilities to access encrypted data. This will go beyond a "sterile debate of backdoors versus no backdoors, to address some of the concrete practical challenges that law enforcement faces."

However, the advanced techniques announced by the commission include technical measures for recovering encrypted data, building on Europol's existing toolbox of decryption capabilities, but the nature of these measures or Europol's capabilities were not disclosed. As EDRi pointed out, these technical measures could mean anything, from state hacking to brute force attacks. Essentially, the commission proposed to fund and develop means to break encryption, somehow without weakening encryption. As Dutch Member of European Parliament Marietje Schaake tweeted, the "commission wants to have its cake & eat it too."

The decision to focus on technical measures, including encryption workarounds, which take the form of government hacking, poses a new set of legal challenges to stakeholders and policymakers in the interim. As Orin Kerr and Bruce Schneier identified in a 2017 report, the law on encryption workarounds is still developing. Many such government hacking capabilities, EDRi argued, are being developed and used without an adequate legal framework and often without respect for national or international human rights safeguards. Europol and Eurojust's joint "First Report of the Observatory Function on Encryption," released in January 2019, takes an important step toward

establishing the necessary legal frameworks for encryption workarounds. However, it concludes that "regulating this domain seems particularly delicate and difficult."

Observers and analysts are wary of the commission's ambition for a European toolbox of alternative investigation techniques, especially considering the aforementioned contradictions among EU agencies and discrepancies across member states. However, European Council on Foreign Relations analyst Stefano Soesanto said that, despite such a toolbox, it would be very difficult for law enforcement to be able to crack the increasingly strong encryption used by foreign technology devices like the iPhone and services including WhatsApp and Telegram. Infosecurity reporter Phil Muncaster added that LEAs would not likely be compelled or willing to share sensitive encryption-cracking forensic tools and expertise across borders without the impetus of legislation, leading him to question the effectiveness of such a shared toolbox.

Related Issues

Other political debates around encryption have touched on proposed EU legislation beyond anti-terrorism and even on issues beyond EU borders.

In 2014, before the string of terrorist strikes in Europe, the European Parliament passed a resolution in response to Edward Snowden's revelation of U.S. mass surveillance activities in Europe. The resolution called on member states, the European Commission, and the European Council to develop and support EU technologies and standards for cybersecurity and encryption, in order to develop greater independence in the IT sector and to protect critical IT infrastructure and citizens' fundamental right to privacy.

In 2017, the early stages of the European "e-evidence" proposal for cross-border access to electronic evidence were intertwined with early policy debates around encryption, for example in the commission's October 2017 communication, and in the commission's first consultation on e-evidence and encryption with industry stakeholders in December 2017. After the first joint consultation on e-evidence and encryption, the commission separated the policy debates and continued with extensive private consultations on the two issues simultaneously. Then, following legislative initiatives in the United States regarding law enforcement's access to data (in particular the Cloud Act), the commission went on to propose a regulation and directive for improved cross-border access to e-evidence in April 2018, stipulating that data should be provided regardless of whether it is encrypted or not.

Encryption has risen as a strong component of the EU's new legal framework to ensure digital privacy for EU citizens through e-privacy (as demonstrated by the E-Privacy Directive) and data protection (as seen in the General Data Protection Regulation). Despite this, encryption has also been caught in the crosshairs of the proposed regulation on e-privacy. While the regulation was intended to ensure the confidentiality of calls, chats, and emails—encrypted or not—it also included

a public interest exception for wiretap provisions, as intended for telecommunications services, which opens questions on how wiretapping surveillance would actually work in digital and, further, encrypted spaces and services.

Outside EU borders, another difficult question facing the EU is about how to manage exports of encryption technology that is considered of dual-use, or capable of being misused for severe human rights violations, terrorist acts, or the development of weapons of mass destruction outside the EU. The EU proposed in early 2018 to modernize its existing dual-use regulation, which was created in response to EU companies providing authoritarian governments with surveillance technology to quell Arab Spring protests. The revision had a stronger focus on human rights and security, but member states pushed back against the new EU export controls, citing conflicting interests in the competitiveness of the EU as a technology exporter.

Outlook

The European Commission is set to continue private consultations on encryption in criminal investigations in the context of its EU Internet Forum with stakeholders such as member states' LEAs, over-the-top service providers (or content providers that distribute streaming media over the internet, such as YouTube), civil society, and academia through 2019. These closed-door conversations will set the tune for public and private EU debates around possible future legislation, to begin with the new European College of Commissioners in late 2019.

Recent EU debates on encryption in response to terrorism have highlighted the collateral risks that legislation to weaken or impose backdoors to encryption poses to European privacy and security. Although vague, the European Council's 2016 decision to focus on assessing encryption issues signals that EU member states have acknowledged the complex nature of the issue, and any next steps toward legislation are to be taken carefully. Observers like Access Now and EDRi cautioned against the narrow focus on finding a solution to encryption as an obstacle to counterterrorism efforts. That focus has fueled political confusion and misunderstanding about the role of encryption technology in the prevention and criminal investigation of terrorism, and has unduly chastised the very same technology that serves to protect the integrity of European critical infrastructure, markets, and societies. These groups, which have cautioned against legislation for law enforcement access to encrypted data, stipulated that the very notion of a policy toward encryption as an impediment to criminal investigations merits more challenge, given the enormous potential of encryption technology to secure Europe compared to the relatively small obstacle it poses to LEAs.

As long as Europe is responding to terrorism and other major crimes, however, the question of whether to regulate encryption and law enforcement's access to data will remain under scrutiny from all sides. Further, as the technology continues to evolve, the debate will have to take into account new technological realities. Without a European Council mandate to legislate on encryption, the

commission's 2017 position to build and support technical measures for addressing and breaking encryption has increased calls for greater transparency and regulations on current government surveillance and hacking capabilities, and for the adoption of adequate safeguards to protect European fundamental rights.

About the Authors

Maria Koomen is a senior program manager at Carnegie Europe.

The author would like to Eric Kind and other, anonymous experts for their review of the manuscript.

Notes

[1] Those countries were Croatia, Hungary, Italy, Latvia, and Poland.

CARNEGIE
ENDOWMENT FOR
INTERNATIONAL PEACE

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

CarnegieEndowment.org