DIGITALEUROPE

16 MARCH 2020

Encryption: finding the balance between privacy, security and lawful data access

Executive summary

Strong encryption is crucial to securing data and communications for individuals, public sector and businesses, including critical infrastructure. These objectives are under assault every day from sophisticated hackers and well-financed criminal organisations.

The technology industry has increasingly introduced built-in and easy-to-use encryption to meet customer requirements and address evolving cybersecurity risks. This trend is likely to continue as enhanced control, e.g. though user-managed keys and full-disk encryption, is considered a driver for user trust. Additionally, the cost of default encryption will likely continue to decrease and users will therefore assume this feature to be granted in their devices and services.[1]

The following conditions are key to getting the best value out of encryption in today's technological and economic landscape:

- Technology providers should be enabled and encouraged to develop and implement strong encryption solutions, tailored to achieve the best possible data security and privacy. Government mandates on the design of technology, such as the creation of 'backdoors,' will impede innovation, hurt the economy and weaken data security and privacy. Encryption also safeguards democracy and human rights by securing election processes and strengthening free speech and journalistic freedom.
- Strong cooperation between the private and public sectors can solve many challenges presented by access to digital evidence. It is imperative that industry and law enforcement authorities continue to cooperate in areas that can help prevent and investigate crimes.

[1] See ENISA, *On the free use of cryptographic tools for (self) protection of EU citizens* (2016), available at https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/enisa-position-on-crypto

DIGITALEUROPE
Rue de la Science, 14A, B-1040 Brussels
T.+32 (0) 2 609 53 10 / www.digitaleurope.org / @DIGITALEUROPE
EU Transparency Register: 64270747023-20

Table of contents

Executive summary 1

Introduction 3

Understanding the value of encryption 3

- Encryption protects critical infrastructure 4
- Encryption protects personal privacy and security 5
- Encryption safeguards democracy and human rights 5
- Exceptional access weakens security 6

Enhancing collaboration between industry and law enforcement 7

- Challenges and opportunities in digital evidence 8
- Easing the burden on law enforcement 9
- 5G 10

Conclusion 11

Introduction

The internet, and the billions of connected devices it enables, has become essential to modern society. Every day, encryption protects privacy and safeguards the critical infrastructure we rely on, from transportation systems to healthcare, energy grids, critical manufacturing plants and financial systems, among others.

Technological advances lead to new threats as the attack surface increases, giving sophisticated adversaries more avenues to infiltrate and take advantage of sensitive data. The safe operation of these services, even more so on upcoming 5G networks, depends on encryption securing and protecting data from hackers and criminals.

According to the World Economic Forum, 'cyber incidents targeting the European business sector have increased since 2018: 61% of businesses reported cyber incidents compared to 45% in the previous year.'[2] ENISA's 2018 *Threat Landscape Report* states that 'mobile threats are expected to increase due to the mobile market growth, users' shift to mobile banking and the upcoming rollout of the 5G mobile standard,' noting for instance that industrial control systems operating critical infrastructure 'will be increasingly targeted by advanced threat actors having … capability and intent.'[3]

In this environment, individuals and organisations have a legitimate expectation that their data, networks, devices and essential services are protected by strong encryption. An informed debate on the most effective use of encryption for jointly pursuing privacy and security and for safeguarding fundamental rights and public interests is therefore needed.

Understanding the value of encryption

The growing importance of data processing in connected devices and in the cloud, including confidential and proprietary data, requires security protections that safeguard the confidentiality, integrity and availability of information for both individuals and organisations, especially in light of the myriad threats to personal data and critical infrastructure. Encryption, alongside other technical and organisational measures, is a critical tool to safeguard data against the worrisome rise in cyber threats.

There is a direct correlation between developments in technology and innovation and an increase in the attack surface. It is estimated that by the end of 2019

[2] http://reports.weforum.org/regional-risks-for-doing-business-2019/regional-profiles/europe/

[3] *ENISA Threat Landscape Report 2018: 15 Top Cyberthreats and Trends*, pp. 27 and 29 respectively

there will be 26.66 billion devices, followed by a significant increase to 125 billion devices by 2030, with 90% of individuals older than six being online.[4] This means more network traffic and ultimately more security challenges.

The World Economic Forum's 2019 Global Risks Report recently identified cyberattacks among the top five global risks, with one-third of the surveyed companies indicating they experienced a cyber incident causing operational impact.[5] Today, the global cost of cybercrime is estimated at about €530 billion.[6]

Attackers are constantly adapting and harnessing new malware, which targets vulnerabilities in the hardware and is more difficult to detect. Encryption is a powerful method that can protect communications and data at rest, in use and in transit.[7] In the last years, for example, ransomware – which encrypts a user's data and is only decrypted by the hacker if the user agrees to a ransom – has been an increasing threat for public administration, public services, small businesses and citizens.

Encryption protects critical infrastructure

In recent years, malware has been used to target critical infrastructure. In March 2019, Norwegian company Norsk Hydro AS, a renewable energy supplier and one of the world's largest aluminium producers, was compromised by the LockerGoga ransomware in a targeted cyberattack. The attack affected large parts of the business, resulting in production stoppages in Europe and the US. Projected costs for the company are up to €35 million.[8]

High-impact attacks, like WannaCry or NotPetya ransomware, swept across a wide range of businesses, hospitals, critical manufacturing and transportation modes, while in 2015 a large-scale cyberattack took out large portions of Ukraine's power grid. Users and organisations that employ cybersecurity best practices and use strong encryption can minimise the risk of these kinds of cyberattacks.

As 5G connectivity spreads, society will become even more dependent on, and intertwined with, wireless communications. Ensuring that sensitive data runs only

[4] https://espas.secure.europarl.europa.eu/orbis/sites/default/files/generated/document/en/ESPAS_Report2019.pdf

[5] http://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf

[6] McAfee, Economic Impact of Cybercrime: No Slowing Down (2018)

[7] McAfee Labs, 2016 Threats Predictions Report, available at https://www.intel.com/content/dam/www/public/us/en/documents/reports/mcafee-2016-threats-and-predictions-report.pdf

[8] Europol European Cybercrime Centre (EC3), 2019 Internet Organised Crime Threat Assessment (IOCTA), available at https://www.europol.europa.eu/sites/default/files/documents/iocta_2019.pdf

over trusted 5G infrastructure will be a herculean task. Encryption will help ensure the confidentiality and integrity of data flowing over networks. This will be critically important as more and more functions rely on network access.

Encryption protects personal privacy and security

Technology providers are challenged every day to protect sensitive user data from numerous sophisticated threats. In the first nine months since the General Data Protection Regulation (GDPR)[9] came into effect, the European Data Protection Board (EDPB) reported data protection authorities (DPAs) received 64,484 breach notifications.[10] That is just a small percentage of a global trend – according to a 2019 report, over four billion personal records were breached in 2019.[11]

Data breaches can expose sensitive information of millions of users and can have potentially life-threatening consequences. Encryption is one of the best tools in protecting users' privacy from malicious actors, as recognised in the GDPR.[12]

Encryption safeguards democracy and human rights

There is increasing recognition that cybersecurity in general, and encryption more specifically, is fundamental to safeguard democracy.

Notably, cyberattacks threaten to undermine the integrity of, and confidence in, electoral processes. According to the NIS Cooperation Group, encryption is a necessary tool to help ensure the integrity and security of EU elections.[13]

Encryption also plays a pivotal role in protecting those who advocate for fundamental human rights. According to the UN Special Rapporteur on Human Rights, '[e]ncryption and anonymity, and the security concepts behind them, provide the privacy and security necessary for the exercise of the right to freedom of opinion and expression in the digital age. Such security may be essential for the exercise of other rights, including economic rights, privacy, due

[9] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 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 (General Data Protection Regulation)

[10] EDPB, *First overview on the implementation of the GDPR and the roles and means of the national supervisory authorities* (2019), available at https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/LIBE/DV/2019/02-25/9_EDPB_report_EN.pdf

[11] See https://us.norton.com/internetsecurity-emerging-threats-2019-data-breaches.html

[12] See Recital 83 and Article 32 GDPR

[13] https://ec.europa.eu/information_society/newsroom/image/document/2018-30/election_security_compendium_00BE09F9-D2BE-5D69-9E39C5A9C81C290F_53645.pdf

process, freedom of peaceful assembly and association, and the right to life and bodily integrity.'[14]

Encryption also protects journalists, providing a measure of security to reporters who expose government abuse or mistreatment of citizens. The 2018 Accra Declaration calls on each UNESCO Member State to '[r]efrain from prohibiting or criminalising the use of encryption and anonymity tools.'[15] Journalistic freedom is an essential component to a democratic society, and encryption is an avenue that allows journalists to continue doing work securely and safely.

Exceptional access weakens security

A backdoor is a feature or defect of a computer system, unknown by the technology provider or undocumented to the user, that allows unauthorised access to data to third parties, e.g. to intelligence agencies. Such exceptional access represents a great risk for security.

For example, Australia's Telecommunications Assistance and Access Act requires providers to insert a vulnerability into all of their products, so long as the government only requests that it be used against certain targets.[16] This fundamentally misunderstands the nature of technology: if a capability to target a user is built, it can be used against *all* users both by well-intentioned law enforcement authorities and malicious hackers, who will inevitably try to gain access.

Mandatory key escrow and key recovery systems to ensure lawful interception have been suggested many times in the past by policymakers.[17] However, such policy options would not only introduce new technological risks to IT infrastructure but could also be easily bypassed by those who wish to keep their communications secret.

Backdoors turn down best practices on security and require increased complexity of IT systems in order to manage vulnerabilities, in turn attracting bad actors such as terrorists, criminals and hacktivists to exploit these vulnerabilities.

---

[14] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye (2015), p. 19, available at https://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session29/Documents/A.HRC.29.32_AEV.doc

[15] https://en.unesco.org/sites/default/files/declaration_accra.2018-05-03.pdf

[16] https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/lawful-access-telecommunications/data-encryption

[17] For background, see Anielle Kehl, Andi Wilson and Kevin Bankston, *Doomed to Repeat History? Lessons from the Crypto Wars of the 1990s* (2015), available at https://static.newamerica.org/attachments/3407-doomed-to-repeat-history-lessons-from-the-crypto-wars-of-the-1990s/Crypto%20Wars_ReDo.7cb491837ac541709797bdf868d37f52.pdf

Applicable law and oversight of exceptional access in multiple countries would further complicate the above-described scenario. As service providers must respond to many thousands of data requests, from different jurisdictions with different legal standards, properly managing and overseeing the use of an exceptional access mechanism would pose a significant challenge given the likely scale of demands.

Maintaining the security of an encryption backdoor that is subject to regular access would be extremely challenging, if not impossible. Additionally, if companies were forced to build an encryption backdoor for rights-respecting countries, they would also face significant pressure to turn over their users' data from countries with less developed democratic standards, which could threaten the human rights of people in those countries.

Finally, encryption remains available through the continuous development of open source software. Forcing companies to weaken the security of their products and services will just drive criminals to use security technologies that are widely understood and available in the public domain or developed in other countries.

Enhancing collaboration between industry and law enforcement

DIGITALEUROPE considers cooperation with public authorities to combat terrorism and crime as a priority when access to data is lawful.

The advancement of technology that provides law enforcement authorities various channels to monitor suspects allows for companies to continue providing robust encryption methods.[18] The volume of data generated by the digital economy has given law enforcement authorities access to more data than at any time in history. In addition, combing with new data mining and processing abilities, authorities are able to gain insights on an unprecedented scale.[19]

Encryption is one element in a complex and ever-changing mosaic of digital evidence that law enforcement agencies must contend with. As new products and services come online, and older ones change, access to certain data often changes or becomes more restricted, or on the other hand new data may

[18] Berkman Centre for Internet and Society, *Don't Panic: Making Progress on the 'Going Dark' Debate* (2016), available at https://cyber.harvard.edu/pubrelease/dont-panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf

[19] Peter Swire and Kenesa Ahmad, *Encryption and Globalisation* (2011), available at https://ssrn.com/abstract=1960602

become available. Understanding these developments and incorporating them into investigative practice is quite difficult.

While some countries have passed laws that allow governments to mandate exceptional access,[20] other laws highlight the benefits of security and enhanced cooperation between law enforcement and industry.[21] DIGITALEUROPE believes that the former, if used to compel law enforcement access, could have dangerous consequences for users around the globe, undermining security and disrupting trust in the digital economy.

Challenges and opportunities in digital evidence

The most pressing digital evidence challenges for law enforcement are understanding what data is available, which providers have it, how to obtain it and how to interpret it.[22] In addition, incomplete legal structures and ineffective cross-border data investigatory processes pose significant challenges for law enforcement agencies within the EU.

These are challenges that are solvable through enhanced collaboration between industry and law enforcement, without compromising the security of millions of technology users.

Typically, intelligence agencies have more tools and techniques available than law enforcement authorities. For example, hacking an end-device – some data is encrypted while in transit but needs to be decrypted in plaintext to be read on the device once received. Furthermore, national authorities have the means to request data (electronic evidence) held by service providers through a combination of national production orders, voluntary disclosure or various mutual

[20] In addition to the Australian Assistance and Access Act, see also the UK Investigatory Powers Act, which allows British law enforcement authorities to order the removal or the redesign of encryption systems through 'technical capability notices.' Through provisions in the law regarding 'equipment interference,' companies may also be forced to insert vulnerabilities into their networks, devices or systems in order to allow access for security services. See http://www.legislation.gov.uk/ukpga/2016/25/contents/enacted

[21] In addition to the GDPR, such laws include Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive), which aims at improving Member States' cyber-security resilience capabilities and establishes security requirements for operators of essential services (e.g. energy, banking and transport) and digital services (cloud, online marketplaces and search engines). In addition, Directive (EU) 2018/1972 establishing the European Electronic Communications Code (EECC) as well as the EU's ePrivacy rules (Directive 2002/58/EC now under reform, COM(2017) 10 final) require that communications services must put in place stringent security measures. Finally, the proposal for an E-evidence Regulation (COM/2018/225 final) aims to make it easier and faster for law enforcement and judicial authorities to obtain electronic evidence to investigate and prosecute criminals and terrorists (see next section below)

[22] CSIS Technology Policy Program Report, *Low-Hanging Fruit: Evidence-Based Solutions to the Digital Evidence Challenge* (2018), available at https://csis-prod.s3.amazonaws.com/s3fs-public/publication/180725_Carter_DigitalEvidence.pdf

legal assistance schemes in cross-border cases.[23] Figures from service providers' transparency reports show that under these frameworks a significant amount of data is being disclosed to law enforcement authorities as part of criminal investigations on daily basis.

Furthermore, a number of Member States are signatories to the Council of Europe's Budapest Convention on Cybercrime, a non-binding resolution which encourages parties to take legislative measures to empower competent authorities to lawfully intercept content data.[24] In cross-border cases, where suspects and evidence may be found in different countries, conflicting national legislation, lengthy procedures for mutual legal assistance (MLA) and competent jurisdiction issues hamper the retrieval of electronic evidence, despite the longstanding cooperation with digital service providers.[25]

Easing the burden on law enforcement

There is a significant amount of important work being done in the EU and internationally to address some of the existing legal and capacity bottlenecks that are frustrating law enforcement authorities' ability to efficiently access data for criminal investigations.

To alleviate some of the practical challenges of the MLA process on law enforcement agencies, both the US and the EU have adopted, or are in the process of adopting, landmark legislation. Industry has supported these efforts, understanding that reducing these barriers will help law enforcement carry out its crucial work.

The US passed the CLOUD Act in 2018,[26] and the EU is currently scrutinising a legislative proposal on e-evidence.[27] Both legislations seek to streamline the process by establishing a legal framework to allow local law enforcement authorities investigating a criminal matter to directly issue a legally binding order to produce data, regardless of where the service provider or data is legally

[23] See the European Commission's impact assessment on the e-evidence legislative proposal (2018), available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018SC0118&from=EN

[24] http://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561

[25] See discussion paper on tackling cybercrime, Meeting of EU Ministers of Justice, Amsterdam 26 January 2016 available at http://english.eu2016.nl/documents/publications/2016/01/22/cybercrime---paper-informal-meeting-ministers-of-justice-and-home-affairs

[26] Clarifying Lawful Overseas Use of Data Act or the CLOUD Act, available at https://www.congress.gov/bill/115th-congress/house-bill/4943

[27] Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters (COM/2018/225 final)

established.[28] A mandate for negotiations on an EU-US agreement has also been adopted[29] and similar work is being done to develop a new protocol to the Budapest Convention on Cybercrime.[30]

In addition, the European Commission has committed significant resources and investment to improve law enforcement authorities' ability to deal with encrypted data. This includes supporting Europol in further developing its decryption capabilities, providing training programmes and toolkits as well as establishing a network of points of expertise and excellence centres for law enforcement authorities to leverage.[31] There is more work to be done here and DIGITALEUROPE's members remain committed to exploring enhanced training for law enforcement.

5G

Lawful interception requirements in the EU have been primarily regulated within national telecommunications legal frameworks. These have been largely operationalised by standards developed by the European Telecommunications Standards Institute (ETSI), the Third Generation Partnership Project (3GPP) or Cable Labs for wireline/internet, wireless and cable systems, respectively.

There is a concern that introducing end-to-end encryption in 5G would prevent legal authorities from accessing necessary data in a similar way to current messaging services operating on 4G networks. However, lawful intercept on new 5G services can be managed through existing technical solutions, and there are no plans for 5G technologies or standards to disable the ability of lawful interception for law enforcement purposes. A lawful interception interface allows the operator to obtain the relevant keys required to decrypt the intercepted traffic in the same way this is already achieved today.

Although encryption of International Mobile Subscriber Information (IMSI) does not prevent law enforcement capabilities such as location tracking, this is currently an optional feature of network operation. The use of IMSI catchers outside the scope of legitimate criminal investigations can be prevented by the IMSI encryption feature and regulators can choose whether operators should

[28] The EU e-evidence proposal would establish a compulsory process, whereby a provider in receipt of a data production order would be required to produce the requested information. The CLOUD Act lifts a blocking statute in the US that prevents providers based in the US from responding to direct requests from foreign law enforcement. US companies can voluntarily produce data in response to a request pursuant to a CLOUD Act agreement.

[29] https://www.consilium.europa.eu/en/press/press-releases/2019/06/06/council-gives-mandate-to-commission-to-negotiate-international-agreements-on-e-evidence-in-criminal-matters/

[30] https://rm.coe.int/t-cy-2019-19-protocol-tor-extension-chair-note-v3/16809577ff

[31] European Commission, Eleventh progress report towards an effective and genuine Security Union (COM(2017) 608 final)

enable this. Any information necessary to facilitate lawful intercept as regards IMSI is handled at the core of the network, which can be accessed via existing lawful interception interfaces.

Conclusion

Privacy and security, both of individuals' personal data and of critical infrastructure, are important preconditions for economic growth and societal benefit. Encryption is a crucial tool to achieve these goals.

Any approach to weaken or grant backdoor access to encryption methods defeats the entire purpose of encryption and undermines users' trust, exposing IT systems to increased risks.

At the same time, it remains vitally important that companies and law enforcement authorities continue to work together, ensuring that authorities have the best methods and access to electronic evidence without weakening or putting strong encryption at risk.

We encourage Member States to remove obstacles in national legislation to Mutual Legal Assistance and to take advantage of the European and international e-evidence negotiations. Companies rely upon the rule of law and a stable political environment where they can freely manufacture and develop their products and architectures, without being required to protect data against access and weaken such protections at the same time.

DIGITALEUROPE is committed to working closely with the EU institutions to encourage opportunities of dialogue between industry, policymakers and authorities.

FOR MORE INFORMATION, PLEASE CONTACT:

Alberto Di Felice

Senior Policy Manager for Infrastructure, Privacy and Security

alberto.difelice@digitaleurope.org / +32 471 99 34 25

Martin Bell

Privacy and Cybersecurity Policy Officer

martin.bell@digitaleurope.org / +32 492 58 12 80

About DIGITALEUROPE

DIGITALEUROPE represents the digital technology industry in Europe. Our members include some of the world's largest IT, telecoms and consumer electronics companies and national associations from every part of Europe. DIGITALEUROPE wants European businesses and citizens to benefit fully from digital technologies and for Europe to grow, attract and sustain the world's best digital technology companies. DIGITALEUROPE ensures industry participation in the development and implementation of EU policies.

DIGITALEUROPE Membership

Corporate Members

Airbus, Amazon, AMD, Apple, Arçelik, Bayer, Bosch, Bose, Bristol-Myers Squibb, Brother, Canon, Cisco, DATEV, Dell, Dropbox, Epson, Ericsson, Facebook, Fujitsu, Google, Graphcore, Hewlett Packard Enterprise, Hitachi, HP Inc., HSBC, Huawei, Intel, Johnson & Johnson, JVC Kenwood Group, Konica Minolta, Kyocera, Lenovo, Lexmark, LG Electronics, MasterCard, METRO, Microsoft, Mitsubishi Electric Europe, Motorola Solutions, MSD Europe Inc., NEC, Nokia, Nvidia Ltd., Océ, Oki, Oracle, Palo Alto Networks, Panasonic Europe, Philips, Qualcomm, Red Hat, Ricoh Europe PLC, Rockwell Automation, Samsung, SAP, SAS, Schneider Electric, Sharp Electronics, Siemens, Siemens Healthineers, Sony, Swatch Group, Tata Consultancy Services, Technicolor, Texas Instruments, Toshiba, TP Vision, UnitedHealth Group, Visa, VMware, Xerox.

National Trade Associations

Austria: IOÖ
Belarus: INFOPARK
Belgium: AGORIA
Croatia: Croatian Chamber of Economy
Cyprus: CITEA
Denmark: DI Digital, IT BRANCHEN, Dansk Erhverv
Estonia: ITL
Finland: TIF
France: AFNUM, Syntec Numérique, Tech in France
Germany: BITKOM, ZVEI
Greece: SEPE
Hungary: IVSZ
Ireland: Technology Ireland
Italy: Anitec-Assinform
Lithuania: INFOBALT
Luxembourg: APSI
Netherlands: NLdigital, FIAR
Norway: Abelia
Poland: KIGEIT, PIIT, ZIPSEE
Portugal: AGEFE
Romania: ANIS, APDETIC
Slovakia: ITAS
Slovenia: GZS
Spain: AMETIC
Sweden: Teknikföretagen, IT&Telekomföretagen
Switzerland: SWICO
Turkey: Digital Turkey Platform, ECID
Ukraine: IT UKRAINE
United Kingdom: techUK