DIGITALEUROPE Views on Encryption

Brussels, 15 July 2016

EXECUTIVE SUMMARY

DIGITALEUROPE as the voice of Europe's digital technology industry expresses its willingness to work closely with the EU Institutions and policymakers to provide valuable knowledge on encryption[1] technology and encourage opportunities of dialogue with industry. As the EU Institutions continue to understand and consider the role that encryption can play in securing the global economy, critical infrastructure and the privacy of individuals, DIGITALEUROPE believes any future actions by policy makers within the field of encryption should focus on:

- **Promoting data security and privacy** - Encryption is fundamental for the economic growth and societal enhancement of the data economy as it allows citizens and organisations to communicate and store information securely and confidentially while protecting data against increasingly sophisticated cyberattacks.
- **Avoiding technology mandates and backdoors** - Government mandates on the design of technology including the creation of backdoors will impede innovation, hurt the economy, and weaken data security and privacy. Technology providers should be enabled to develop and implement encryption solutions tailored to achieve the best possible data security and privacy.
- **Encouraging judicial cooperation between Member States** – Member States must overcome conflicts in national legislation, lengthy procedures for mutual legal assistance and competent jurisdiction issues.
- **Enhancing collaboration between industry and law enforcement** – Strong cooperation is needed between the private sector and public sector when access to data is needed for law enforcement purposes. Industry stands ready to partner in areas which could be more effective in identifying 'malicious' actors.
- **Mitigating risks in the Internet of Things and the Cloud** - Encryption protects sensitive and confidential data in the Cloud and in the Internet of Things environment, where it becomes a mitigating factor for security, privacy and safety risks and an accountability measure.
- **Ensuring the free flow of data in the Digital Single Market** - Encryption guarantees secure interaction among devices, network, supporting infrastructures and users.
- **Avoiding restriction in trade agreements** – Future EU trade agreements should avoid restrictions on the import, use and sale of commercial cryptographic goods.
- **Promoting innovation, research and investments** - Promote the use of EU funds to increase research and investment into stronger private sector driven encryption solutions along with emerging/evolving technologies (e.g. blockchain) to leverage the opportunities offered by these new technologies.

[1] While this paper focuses on encryption technology, we wish to stress that this is only one way to ensure the security of data systems. We caution against technology mandates and support a technology neutral approach to technologies aimed at increasing privacy and security of systems. Encryption is only one solution of many.

1. Introduction

In contemporary society, confidentiality, integrity and availability of information are considered key security objectives for both public and private sectors. We live in a **data economy** where people make use of billions of electronic devices, which are connected among themselves and with the cloud to create, transfer and store data. Large sets of data ("big data") are processed and analysed to further improve people's knowledge and devices' performances.

In this environment, individuals and organisations have a legitimate expectation to limit access to data by non-authorised parties (**confidentiality**), to keep data accurate and consistent (**integrity**) and to avoid any data loss (**availability**). In other words, data privacy and data security represent a societal priority. They can be pursued through cryptographic tools and therefore encryption helps to ensure privacy and security for communications, technology products and digital services. In particular, device integrity is complementary to data integrity, because the security of all end-points and networks in use represents an essential precondition for trusted computing (see section 3 b below).

So far, the complexity of technical aspects may have impinged on an open debate around encryption. In this paper, DIGITALEUROPE focuses on data encryption and explores policy areas related to technology, with the aim of landscaping the major issues where policymakers' awareness is crucial for future technological developments and societal benefits.

DIGITALEUROPE stands ready to support policymakers in developing an informed debate on the most effective use of encryption for jointly pursuing privacy and security and for safeguarding fundamental rights and public interests.

2. Encryption: basic and benefits

To better understand the context for policy decisions regarding encryption we will describe a few cryptographic concepts and defer to primers available on the market for a detailed analysis of cryptography and encryption.[2]

Cryptography is the study of techniques for secure communications while encryption is the process of encoding information in such a way that only authorised parties can read it. More precisely, an ordinary text (called **plaintext**) can be transformed into an unreadable format, an encrypted text (called **cyphertext**), which needs a key to be decrypted. An **algorithm** (cypher) contains a precise set of instructions on how to scramble (or unscramble) data: secret messages will be unlocked using a **key** (a complex sequence of alphanumeric characters).

Let us take the following simple sentence "The weather in Brussels is often cloudy" as an example to create a very simple cypher with a key. We can pick a date (31 March 2016, 310316 will be our key) and write these digits below our sentence:

The	*weather*	*in*	*Brussels*	*is*	*often*	*cloudy*
310	3163103	16	31031631	03	16310	316310

[2] Useful primers for cryptography/encryption are F. Piper, S. Murphy "Cryptography. A very short Introduction", Oxford University Press, 2002 and C. Cobb, "Cryptography for Dummies", John Wiley & Sons, 2004

To transform the plaintext into cypher text, each letter needs to be shifted back in the alphabet (ABCDEFGHIJKLMNOPQRSTUVWXYZ) by the number of spaces indicated by the digit below each letter (e.g. T shift 3 spaces and becomes Q). The encrypted message would read like this:

QGE TDUQGEO HH YQUPRYIR IP NZNDN ZKIRCY

To decrypt the cyphertext the recipient will need to know the key (310316) and be aware of the cypher ("shift forward as many letter as the digit"). As long as this information is made available only to our intended recipient, the message remains secret.

Cryptographic algorithms are used for several concrete applications but with a much higher degree of complexity. In fact, the computing environment offers many ways to operate additional scrambling and heavy computation. In both the fictitious example provided and in the real deployment of cyphers, encryption is useless if the cypher key is not well protected and secret, because the algorithm becomes breakable and the encrypted information accessible.

Key types and management represent crucial aspects for individuals and organisations in order to deploy effective security. Some forms of encryption use one key to transform plaintext into cyphertext and vice versa. This **symmetric encryption** has been used since the 1960s until now with substantial improvements in the sophistication of the protocols. **Asymmetric encryption** uses a key pair: one key is public and is used to encrypt the text while the other one is private and can decrypt it. This solution was developed in the 1970s but achieved a broader commercial use in the 1990s and still remains a fundamental way to encrypt data. **Hybrid encryption** combines features and procedures of the other two cryptographic architectures.

Today **end-to-end encryption** allows secure data transfer among end-point devices. In fact, in this system of communication, only people communicating can read the messages, and no one in-between (including telecom providers, Internet providers, companies that run messaging services) have access to the cryptographic keys to decrypt the conversation.[3] This technology is increasingly implemented in instant messaging and telephony applications. Many business models are based upon increasing consumer demand for data protection. Limiting the number of actors aware of the keys reduces also the targets for cyberattacks; notwithstanding, endpoint security remains a challenge also in this context because devices can be hacked.

However, at the fundamental technology level, the importance of robust encryption does not change if this is operated on **data at rest** (while stored e.g. in a data centre or an endpoint device), **in transit** (while transferred from one repository to another) or **in use** (while processed e.g. in the cloud or in a smartphone). The same cryptographic algorithms are frequently used but implementations are different and influenced by other factors (see below section 3 a).

At present, encryption is increasingly embedded in every day technologies and helps ensuring secure access to services (e.g. logons, passwords, ATMs, banking online, e-commerce applications), privacy of individuals' and businesses' communications (instant messaging, virtual private networks, webmail) as well as protection of commercial contents (digital rights management for copyrighted material such as DVDs).

Tangible **privacy and security benefits** result from the use of encryption because it mitigates risks related to data confidentiality, integrity and availability. Data is more likely to be kept secret, not modified and accessible only by the user. Cryptographic tools can also improve procedures for user authentication (preventing access from

[3] For reader's reference: http://www.wired.com/2014/11/hacker-lexicon-end-to-end-encryption/

unauthorised actors) and guarantee the complete execution of instructions (so called non-repudiation), as in the case of digital signatures. Technology has developed multiple ways to minimise the damage of a cyberattack, as in the case of some modern cryptographic tools which generate "session keys" used only one time: even in case of successful cyberattacks, past communications cannot be disclosed and therefore remain protected ("forward secrecy").

3. Technologies and encryption from a privacy and security policy perspective

To open up the policy debate on encryption, we identified some areas where cryptographic tools are used to improve privacy and security of products and services. The interest in these cryptographic applications is cross-cutting - citizens, public administration and private sector increasingly embrace and trust encryption - therefore current and future use cases are particularly relevant to policymakers in their effort to find appropriate policy solutions to societal challenges and opportunities.

The actual **threat landscape** is worsening as the cyberattack surface is growing: more users, more data, more connected devices (6.4 billion by the end of 2016[4], 50 billion by 2020[5]), more network traffic, therefore more security challenges (in 2016, around 500 thousand new threats a day, over 360 every minute[6]). Data corruption, sniffing of confidential data, unauthorised access to sensitive data, identity theft, data loss or destruction are unfortunately typical threat scenarios. Attackers are experimenting with new malware, which targets vulnerabilities in the hardware and which is more difficult to detect. Hence, encryption can help better protect communications and data at rest, in use and in transit[7]. In the last years, for example, ransomware[8] has been an increasing threat for public administration, public services, small enterprises and citizens: this malicious software (malware) restricts user access to data stored in the infected device. This restriction (often data is encrypted by the attackers) can be unlocked only after the payment of a ransom to the cybercriminals. It is reasonable to infer that users encrypting their sensitive data can minimise the risk of this kind of cyberattacks.

In this context of increasing cybersecurity challenges, the access to data by law enforcement authorities (section 3 a), the data economy taking advantage of the Cloud and the Internet of Things (section 3 b), encryption in trade agreements (section 3 c) and future applications of blockchain technology (section 3 d) are three areas where encryption will make a difference in ensuring growth and societal benefit.

DIGITALEUROPE acknowledges the worrisome rise in cyber threats and considers encryption as a valuable tool alongside other technical and organisational measures to safeguard data against unauthorised or unlawful access. DigitalEurope encourages policymakers to promote the use of encryption, which will protect privacy while also protecting national and critical infrastructure security.

[4] "Gartner Says 6.4 Billion Connected Things Will Be in Use in 2016, Up 30 Percent From 2015" retrieved at http://www.gartner.com/newsroom/id/3165317

[5] D. Evans, "The Internet of Things. How the Next Evolution of the Internet Is Changing Everything", Cisco, 2011

[6] Keynote speech by C. Young (Intel Security) at RSA Conference 2016 (San Francisco, March 2016)

[7] McAfee Labs, "2016 Threats Predictions", Intel Security, 2016

[8] After being covertly installed on a computer, this malware restricts access to the computer system and, in some cases, encrypts all files. The user is then asked to pay a ransom to the ransomware operators to remove the restriction.

a) Access to data by law enforcement agencies

The debate on whether technology could neutralise investigative capabilities of law enforcement authorities dates back to the 1990s. Since then, police and government agencies claimed to suffer from "**going dark**".[9] Even if today the adoption of encryption can make it harder to intercept data, technological trends show that there will be other channels for law enforcement authorities to monitor suspects.[10]

Nowadays, access to data by law enforcement agencies is reached through **lawful interception** capability requirements, which have been implemented worldwide by countries using requirements and standards developed by the European Telecommunications Standards Institute (ETSI), the Third Generation Partnership Project (3GPP) or Cable Labs organisations, respectively for wireline/Internet, wireless and cable systems. Typically, intelligence agencies have more tools and techniques available than law enforcement authorities e.g. hacking an end-device and accessing data because some data is encrypted while in transit but needs to be decrypted in plaintext to be read on the device once received.

Lawful interception is regulated at national level in all EU Member States. Almost all of them joined the **Budapest Convention on Cybercrime (2001)** by the Council of Europe, a non-binding resolution, which encourages Parties to take legislative measures to empower competent authorities to lawfully intercept content data.[11] In cross-border cases, where suspects and evidence may be found in different countries, **conflicting national legislation, lengthy procedures for mutual legal assistance and competent jurisdiction issues** hamper the retrieval of electronic evidence, despite the longstanding cooperation with digital service providers.[12]

Public and private actors share the common goal of security in cyberspace. However, recent proposals to revise legislation put forward by some Member States have drawn public attention to encryption-related issues. There should not be a trade-off between data protection and security, both should be pursued in parallel.

The National Assembly in **France** has recently amended a counterterrorism bill aggravating criminal sanctions for private companies refusing to provide authorities with data protected by encryption in the course of investigations on organised crime and terrorism.[13] The obligation for digital services providers to hand over decryption keys or to unlock encrypted data following a request by law enforcement is also foreseen in the French surveillance law adopted in 2015. In the **United Kingdom**, a draft Investigatory Powers Bill is at the time of writing under parliamentary scrutiny. The Bill, as currently drafted would allow law enforcement authorities to order the removal or the redesign of encryption systems through so-called 'Technical Capability Notices'. Through provisions in the Bill regarding 'Equipment Interference', companies may also be forced to insert vulnerabilities into their networks, devices or systems in order to allow access for the security services; in effect weakening the

[9] James B. Comey, Federal Bureau of Investigation Direction in a speech at Brookings Institution, Washington DC on 16 October 2014, accessible at https://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course

[10] M. Olsen et alia, "Don't Panic. Making Progress on the Going Dark Debate", The Berkman Centre for Internet and Society, Harvard University 2016

[11] The text is available at: http://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561

[12] 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

[13] Amendment available at: http://www.assemblee-nationale.fr/14/amendements/3515/AN/90.asp retrieved on 21 March 2016

security of their encrypted products. Additionally, the law could ban encryption stronger than 64-bit key.[14] Nonetheless, **European Commission**'s Vice-President Ansip has taken a firm stance against weak encryption[15]; the Dutch Government, at the beginning of its EU Presidency, stated that it is not necessary for the **Netherlands** to adopt restrictive measures regarding the development and the use of encryption[16]; and in France the Undersecretary of State for digital issues referred publicly to backdoors as a "vulnerability by design".[17]

With reference to access to encrypted data, it is largely acknowledged by academia and industry that it is not possible to give exceptional access to law enforcement authorities through backdoors[18] without creating **unacceptable risks for security**. To do so would mean that best practices on security, such as strong encryption, would be turned down; the complexity of the system would have to increase in order to manage vulnerabilities, and this would attract bad actors such as terrorists, criminals and hacktivists who would try to exploit them. Additionally, applicable law and oversight of exceptional access in multiple countries would further complicate the above-described scenario.[19]

Mandatory key escrow and key recovery systems to ensure lawful interception have been suggested in the past by policymakers.[20] However, such policy options would not only introduce new technological risks to the IT infrastructure, but could also be easily bypassed by those who wish to keep their communications secret. In fact, **data encryption remains available** through the continuous development of open source software to encrypt data. Forcing companies to weaken the security of their products will just drive criminals to use security technologies that are widely understood and available in the public domain or developed in other countries. Additionally, **restricting the use of encryption in commercial products could heavily damage the IT industry** [21] as it would weaken security throughout while failing to achieve the policy purpose.

The technology industry moves fast and depends on rapid innovation to meet customer requirements and address evolving cybersecurity risks. Technology companies have increasingly introduced built-in and easy-to-use encryption: we can expect this trend to continue because **enhanced users' control** is a driver for consumers' **trust in technology**. User-managed keys and full-disk encryption of devices will continue to be useful for securing data and communications for individuals, public sector and businesses. Additionally, we can reasonably predict that the cost of default encryption will continue to decrease and therefore consumers will assume this feature to be granted in their devices.[22]

[14] The key size (or length) is represented by the number of bits in a key used by the cryptographic algorithm, therefore with a key of length "n" bits, there would be 2^n possible keys. Limitation to key size are linked to the capability of law enforcement authorities to break the keys up to a certain size.

[15] "Ansip slams encryption backdoors" published on Politico.eu on 11 March 2016

[16] The position paper is available at the Dutch House of Representatives website: https://www.tweedekamer.nl/kamerstukken/brieven_regering/detail?id=2016Z00009&did=2016D00015

[17] http://www.numerama.com/politique/138689-chiffrement-le-gouvernement-rejette-les-backdoors.html

[18] A backdoor is a feature or defect of a computer system - unknown by the technology provider or undocumented to the user - that allows unauthorized access to data to third parties e.g. to intelligence agencies.

[19] H. Abelson et alia, "Keys Under Doormats: mandating insecurity by requiring government access to all data and communications", Massachusetts Institute of Technology (MIT), Journal of Cybersecurity vol. 1(1), 2015

[20] New America Foundation, "Doomed to Repeat History: Lessons from the Crypto Wars of the 1990s", 2015

[21] ENISA, "On the free use of cryptographic tools for (self) protection of EU citizens", 2016

[22] Moore's law: Gordon Moore found in 1965 that the computing would dramatically increase in power, and decrease in relative cost, at an exponential pace.

DIGITALEUROPE acknowledges the mission of law enforcement authorities therefore considers cooperation with public authorities to combat terrorism and criminal organisations as a priority when access to data is lawful.

DIGITALEUROPE encourages Member States to remove obstacles in national legislation to mutual legal assistance. 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 provide it at the same time.

DIGITALEUROPE does not endorse any effort by governments to weaken technology nor supports technology mandates that are likely to impede needed innovation: any backdoors built into encryption would undermine the value of technology as well as individuals privacy and security.

Additionally, DIGITALEUROPE finds that the current debate is distracting efforts to take advantage of other information such as "digital exhaust" to identify and counteract bad actors (unencrypted metadata, e.g. location data, phone records).

b) Data encryption in Cloud Computing and the Internet of Things

Individuals and organisations are storing more and more information in the cloud. **Cloud computing** has different models for services (cloud as an infrastructure, as a platform, as a software) and deployment (public, private, community, hybrid).[23] However, in all these configurations, **data security and privacy** are the paramount goals of any cloud provider and the major needs for any cloud user. Encryption proved to be a baseline technology, and is nowadays essential to protect sensitive data in the cloud environment. Governments, public administrations, and public and private operators of essential services (e.g. hospitals, airports, energy and water suppliers, banking and finance sector) have increasingly shifted their databases and operations on directly- or third party- owned and managed cloud. Public administration and governments, for instance, leverage the flexibility, the efficiency and the cost reduction of cloud computing technology to deliver **e-government services**.[24]

Sensitive data concerning citizens and consumers are increasingly processed and stored in the cloud; the same has happened for organisational **confidential and proprietary data**. This trend entails also higher expectations in terms of confidentiality, integrity and availability for that information. Additionally, due to the centralised nature of cloud computing architecture, cybercriminals focus their attacks on data centres and therefore strong encryption of data can mitigate the risk of disclosure of information or limit the damage if data is accessed or stolen.

In December 2015 the EU Institutions reached an agreement on the **Network Information Security Directive** which aims at improving resilience capabilities by Member States in the field of cybersecurity and establishes security requirements for private operators of essential services (e.g. energy, banking, transport) and digital services (cloud, online marketplaces, search engines). These requirements are going to be set through implementing acts

[23] P. Mell, T. Grance, "The NIST Definition of Cloud Computing", National Institute of Standard and Technology, 2011

[24] S. Hashemi et alia, "Using Cloud Computing for E-Government: Challenges and Benefits" World Academy of Science, Engineering and Technology International Journal of Computer, Electrical, Automation, Control and Information Engineering Vol.7, No.9, 2013

and encryption might be considered amongst the technical and organisational security measures to guarantee security and privacy by essential or digital service providers.

In a similar manner, the same need for EU legislative harmonisation in the cybersecurity space led to specific provisions on data security also in the upcoming **General Data Protection Regulation**: the new data protection framework will put some obligations on data controllers and processors regarding risk-based security measures for data processing as well as breach notifications. Indeed, privacy cannot exist without appropriate levels of security.

Our interpretation of these developments is that to ensure the protection of data, more data has to be processed for security purposes, in order to detect malware or loss of integrity. The result of prevention and malware detection activities shall be compared across different regions of the world and therefore **free flows of data** are essential to guarantee accurate analysis of the ecosystem. At the same time, free flow of data is essential for the **Internet of Things** (IoT) because it relates to the possibility for devices to exchange data for computational purposes. In fact, with IoT we refer to the network of physical objects that enables these objects to collect and process data. IoT can be described as a "system of systems", as a complex, ubiquitous, dynamic environment where the physical and the cyber dimensions are intertwined and where objects communicate wireless among themselves.[25]

In the IoT ecosystem, "things" can be smartphones, computers, sensors, healthcare devices, vehicles, buildings, grids and any kind of "smart" item with software and internet connectivity. In some cases, electronic devices have constrained capabilities due to limited power supply, storage, connectivity, or computing capabilities. However, if one component, one node of the network is compromised by a cyberattack, the whole IoT network could suffer seriously from this. Encryption proved one of the crucial tools to preserve and enhance security of the whole system, but cryptographic algorithms and their implementation need to be adapted for devices with constrained resources or such environments as massive data sets, that are sometimes the result of environment data collection via sensors.

Lightweight encryption is a technology area that extends the limits of traditional cryptography and implementation techniques in the IoT environment. In fact, lightweight encryption is the implementation of encryption in environments that have very limited resources in terms of memory, computing power, and battery supply. The efforts made in this direction (e.g. on the chip size or the energy consumption) are instrumental in extending the advantages of stronger encryption to small devices and low power environments to ensure endpoints and aggregation systems do not become single points of failure in various IoT ecosystems. Advances in this area will permit the operators to run lightweight encryption implementations without compromising effective data protection and security.[26]

Networks, devices, supporting infrastructure such as Cloud and users are important components of the typical IoT environment. In this context, a "silo approach" to manage risks is not viable, due to the **interplay of security, privacy and safety**. These aspects need a risk composition to enhance trust in IoT by users. Encryption can play a prominent role in addressing multiple risks in different IoT sectors. If a connected toy used by kids is hacked because of insufficient security measures, it can be used to violate privacy in the home and can be a serious threat

[25] International Telecommunication Union (ITU), Recommendation Y.2060, 2012 defines Internet of Things (IoT) as ”A global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies."

[26] More information in M. Katagi, S. Moriai, "Lightweight Cryptography for the Internet of Things" or in the NIST Lightweight Cryptography project run by NIST http://www.nist.gov/itl/csd/ct/lwc-project.cfm

to the physical safety of children. In a similar way, autonomous driving cars will be connected among themselves and will be able to exchange encrypted data. Strong encryption will mitigate the risk for access to drivers' personal data by cybercriminals and especially for drivers' safety threats such as car accidents. It appears evident that flaws in security will likely affect privacy, safety and, overall, the entire reliability of the ecosystem.

The complexity described above does not affect the concept of defective product and its related legislation[27], but surely brings a further element into the policy debate on **liability in the IoT ecosystem**, to encourage stronger security measures such as encryption, which will have beneficial spillovers also on privacy and safety. While Internet of Things technologies are developing, a flexible and future-proof approach should privilege a proactive role of companies in risk analysis and risk management. The use of encryption, in this perspective, could be seen as an accountability measure by companies with regard to security, privacy and safety. Contractual clauses will continue playing an important role in defining liability of product developers within the value chain, especially in the B2B (business-to-business) framework.

End-to-end encryption solutions are security features already in place which could be further deployed and developed in the IoT ecosystem, because they secure the flows of data among devices. In fact, data in transit can be read only by end users (who own the keys to decrypt), avoiding access by third parties. As stated in our introduction, security issues at endpoint devices need to be addressed: robust multifactorial authentication mechanisms can help in preventing and pushing back common cyberattacks (e.g. the combination of a PIN code with fingerprints, or retinal pattern and a security token). However, end-to-end solutions are not basic and easy to implement in an IoT space, especially for small and medium enterprises, because they entail the full encryption of networks, devices and supporting infrastructures. **Encryption can be ubiquitous but its use is not universal.**

DIGITALEUROPE encourages policymakers to support encryption as a technology ensuring data privacy and data security in the Cloud and in the IoT, where sensitive and confidential data is increasingly processed. DIGITALEUROPE recognises that recent legislation considers security requirements a key feature of digital products and services and their application crucial for maintaining an overall high level of security.

In securing data storage and transfer, companies expect data to flow freely in the Digital Single Market. DIGITALEUROPE believes encryption can secure the interaction among devices, network, infrastructures and users.

In a complex IoT environment, DIGITALEUROPE acknowledges the importance of encryption as a mitigating factor for security, privacy and safety risks, which cannot be managed in separate silos anymore. If the interaction of privacy, security, safety and reliability can have an impact on liability, encryption could be seen as an accountability measure to prevent damages to users.

[27] Product Liability Directive (85/374/EC)

c) Encryption in trade agreements

In order for encryption to provide as high a level of security and privacy as possible, it is paramount that no level of the ICT industry's **global supply chains** becomes subject to legal requirements that would lower or weaken the level of encryption, (e.g. through mandated use of certain cryptographic algorithms). DIGITALEUROPE believes that in order to offer the products with the highest security standards, the import, use and sale of commercial cryptographic goods should be largely unrestricted.

As the first trade agreement to incorporate provisions on the trade in cryptographic goods, the Trans-Pacific Partnership (TPP) agreement bans TPP parties from requiring makers or suppliers of goods that use encryption for commercial applications (e.g. cell phones, game consoles or routers) to transfer or disclose proprietary encryption technology, production processes or other information to government or a domestic partner, or to partner with a domestic partner, or to use a particular type of encryption, as a condition of being able to make, import, sell, distribute or use these goods. A separate provision bars any TPP party from prohibiting the importation of 'commercial cryptographic goods' (i.e. goods that implement or incorporate cryptography, sold to the general public).

DIGITALEUROPE fully supports the inclusion of equivalent provisions in other trade agreements, notably the Transatlantic Trade and Investment Partnership (TTIP), as a core element of making sure such trade agreements serve the needs of the 21st century digital economy and enable the secure use of ICT technologies.

d) Emerging technologies: blockchain

Blockchain represents a research area and emerging technology of considerable interest. In recent years, it has gained prominence because it underlies some virtual currencies, or cryptocurrencies[28], which rely on cryptographic tools to confirm transactions. However, blockchain technology is considered a game changer because it may be exploited for many applications across very different sectors.

Blockchain is a distributed database that maintains a continuously-growing list of data records hardened against tampering and revision. As a public ledger it accounts for all the transactions which are recorded and stored on its blocks, through cryptographic algorithms, forming a chain of timestamped events. It facilitates the transfer of ownership of a digital asset and provides a permanent, irreversible record of transactions without need for oversight by a third party.

Industry is exploring **several applications** for blockchain, from more secure and faster financial transactions to non-repudiable and self-enforceable smart contracts, to safer and reliable data storage to robust management of digital rights and digital identities: all of these use encryption. Asset or data ownership, transaction records, user identity or data integrity could benefit from the use of blockchain technologies. Additionally, a clear record of transactions performed could improve solutions for regulatory compliance and reduce compliance costs.

Similarly, governments and public administration may benefit from blockchain technology in developing **new e-government services:** integrity, reliability, verifiability, traceability of information recorded on blocks open to applications such as public databases, civil registries, notary services, enforcement of property rights, incentive

[28] For readers' convenience we refer to https://en.wikipedia.org/wiki/List_of_cryptocurrencies

schemes as well as voting systems. All these new services would have the twofold benefit of enabling governments and public administration to be more transparent and more accountable before citizens.

DIGITALEUROPE deems blockchain technology to be enabler of newer approaches to encryption and integrity, and a driver for transparency and accountability both for the public and the private sectors. DIGITALEUROPE encourages policymakers to prioritise research and investments in this field to leverage the opportunities blockchain offers.

4. Conclusion

Creating awareness around encryption from a privacy and security policy perspective is the first step to open up the discussion at EU and national levels. DIGITALEUROPE confirms its willingness to work closely with the EU Institutions and policymakers to provide valuable knowledge and to encourage opportunities of dialogue with industry. Privacy and security are important preconditions for economic growth and societal benefit and encryption is a crucial tool to achieve these goals.

--
For more information, please contact:
Damir Filipovic, DIGITALEUROPE's Director (Digital Enterprise & Consumer Policy)
+32 2 609 53 25 or damir.filipovic@digitaleurope.org

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’s members include 62 corporate members and 37 national trade associations from across Europe. Our website provides further information on our recent news and activities: http://www.digitaleurope.org

DIGITALEUROPE MEMBERSHIP

Corporate Members

Airbus, Amazon Web Services, AMD, Apple, BlackBerry, Bose, Brother, CA Technologies, Canon, Cisco, Dell, Dropbox, Epson, Ericsson, Fujitsu, Google, Hewlett Packard Enterprise, Hitachi, HP Inc., Huawei, IBM, Ingram Micro, Intel, iQor, JVC Kenwood Group, Konica Minolta, Kyocera, Lenovo, Lexmark, LG Electronics, Loewe, Microsoft, Mitsubishi Electric Europe, Motorola Solutions, NEC, Nokia, Nvidia Ltd., Océ, Oki, Oracle, Panasonic Europe, Philips, Pioneer, Qualcomm, Ricoh Europe PLC, Samsung, SAP, SAS, Schneider Electric IT Corporation, Sharp Electronics, Siemens, Sony, Swatch Group, Technicolor, Texas Instruments, Toshiba, TP Vision, VMware, Western Digital, Xerox, Zebra Technologies, ZTE Corporation.

National Trade Associations

Austria: IOÖ
Belarus: INFOPARK
Belgium: AGORIA
Bulgaria: BAIT
Cyprus: CITEA
Denmark: DI Digital, IT-BRANCHEN
Estonia: ITL
Finland: FFTI
France: AFNUM, Force Numérique, Tech in France
Germany: BITKOM, ZVEI
Greece: SEPE
Hungary: IVSZ
Ireland: ICT IRELAND
Italy: ANITEC
Lithuania: INFOBALT
Netherlands: Nederland ICT, FIAR
Poland: KIGEIT, PIIT, ZIPSEE
Portugal: AGEFE
Romania: ANIS, APDETIC
Slovakia: ITAS
Slovenia: GZS
Spain: AMETIC
Sweden: Foreningen Teknikföretagen i Sverige, IT&Telekomföretagen
Switzerland: SWICO
Turkey: Digital Turkey Platform, ECID
Ukraine: IT UKRAINE
United Kingdom: techUK