Brussels, April 11 2018

ARTICLE 29 Data Protection Working Party

Statement of the WP29 on encryption and their impact on the protection of individuals with regard to the processing of their personal data in the EU

The data protection authorities of the European Union, represented in the Article 29 Working Party (WP29), consider that the availability of strong and efficient encryption is a necessity in order to guarantee the protection of individuals with regard to the confidentiality and integrity of their data which are the elementary underpinning of the digital economy. Any obligation aiming at reducing the effectiveness of those techniques in order to allow law enforcement access to encrypted data could seriously harm the privacy of European citizens.

Taking into account the pressing need to balance between different public interests, like trust in digital services on one hand, and the effective prosecution of crimes on the other, and to safeguard the individual right to confidentiality and privacy, the Working Party communicates the following key messages on this issue.

1. Strong encryption is required to ensure a secure, free flow of data between citizens, businesses and governments.

The widespread use of services enabled by information and communication technologies has made encryption a critical and widely-used tool to help ensure that data are secured. Properly-implemented encryption using appropriate algorithms offers a reasonable guarantee that activities like buying goods online, filing one's taxes, using banking services, sending or receiving emails or making an appointment with a physician can be done securely.

Without encryption, individuals' privacy and security can be compromised every time they wish to undertake those everyday activities. Indeed, use of encryption techniques as a means of guaranteeing confidentiality and integrity of data and user authentication has become an indispensable prerequisite for the normal functioning of these infrastructures and of the digital services offered over them, and is now used by many data controllers. Encryption is therefore absolutely necessary and irreplaceable for guaranteeing strong confidentiality and integrity when data are transferred across open networks like the Internet, or stored in mobile devices like smartphones. This encryption should ideally always cover the entire communication, from the device of the sender to that of the recipient (end-to-end-encryption).

To be dependable, the broadest public availability of state of the art, strong and reliable encryption needs to be promoted to allow for public scrutiny. Doing so enables researchers to study such software to assess and improve its efficiency and robustness, which in turn helps industry to implement these techniques for reliable and trustable services. With regard to this, emerging quantum cryptography capabilities should be taken into consideration.

There is also a public interest in the implementation of encryption. Securing personal data in transit and at rest is a cornerstone of the trust we all need for digital services, so as to enable innovation and growth for our digital economy.

2. Backdoors and master keys deprive encryption of its utility and cannot be used in a secure manner.

Encryption also allows to conceal criminal activities. This presents a challenge for law enforcement agencies that seek to access communications or data in those cases.

Some consider that the need for law enforcement to access the data of suspected criminals can be satisfied by implementing "backdoors" (i.e. vulnerabilities secretly implemented in a particular software by its developer) or "master keys" (i.e. keys allowing the decryption of every message encrypted with a specific software) in encryption software. This could mean that developers of these technologies would be required to include and make available such facilities to law enforcement, allowing them to decrypt and access the plaintext data.

However, the mathematical foundation of cryptology does not provide the basis for a secure backdoor, and numerous examples in history have shown that master keys and backdoors cannot be kept secure, even by major law enforcement agencies[1] or by companies specialized in key management:

- The widely-reported leak of Transportation Security Administration (TSA) keys, a set of physical keys which open most of the suitcases on the planet, supposedly accessible only to TSA personnel, meaning that anyone can open a TSA lock.
- The global WannaCry cryptolocker that infected tens of thousands of computers in hundreds of organisations worldwide used tools designed to exploit existing vulnerabilities in file sharing protocols. These tools, created by a major national security agency, were leaked to the public and then used by criminals to create the WannaCry cryptolocker.
- The compromise of the private keys of a major certificate provider that led to the breach of several certificates of widely-used services and the compromise of the email accounts of activists in Iran.

Manufacturers and service providers themselves acknowledge that they could not ensure the security of backdoors that would be accessible only to them[2]. This illustrates the technological risks that arise from the reliance by organisations on their ability to keep software vulnerabilities secret.

Encryption software is also used on a worldwide scale. To be effective, backdoors and master keys would therefore have to be exchanged between law enforcement agencies on a worldwide scale. This would lead to their widespread dissemination and thus increase the risks of them being compromised.

Without strong and efficient encryption, data of citizens, businesses and governments are at risk. Given the importance of the security of everyday services – upon which our individual lives, businesses and governments increasingly rely – any decrease in the protection offered by encryption will lead to even greater damages than that which law enforcement access to encrypted data might aim to prevent.

Moreover, imposing backdoors and master keys on law abiding citizens and organisations would not be an effective measure against criminals since they would continue to use or adapt the strongest state of the art encryption to protect their data, keeping them safe from law enforcement access. As a result, backdoors and master keys would only harm the honest citizen by making their data vulnerable.

[1] EUROPOL and ENISA's position : https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/on-lawful-criminal-investigation-that-respects-21st-century-data-protection

[2] Apple 's position : https://www.apple.com/customer-letter/

3. Law enforcement agencies already have a number of legal powers and targeted tools to address the challenge of encryption, allowing them to access the data they need to investigate and prosecute criminals.

Law enforcement agencies in EU Member States can be legally empowered in other ways to obtain access to data otherwise encrypted, including personal data, for investigations in targeted circumstances. For instance, depending on the laws of individual Member States, those agencies may have the power to:

- Access communications metadata and unencrypted data held by data controllers.
- Use social engineering to infiltrate criminal organisations.
- Require alleged criminals and/or persons of interest to provide their encryption key.
- Use targeted interception tools such as IMSI catchers (a tool designed to intercept mobile communications in its vicinity), or intercept specific electronic communications by accessing electronic communications providers' networks.
- Use specific and targeted tools to guess or intercept a password, access documents and/or record keystrokes before encryption on the sender's device, or after decryption by the recipient.
- Obtain individual's encryption keys that are held by data controllers or key escrow services.

Even though these powers raise serious privacy concerns and require significant legal and technical safeguards, they appear more proportionate and less dangerous than master keys and backdoors.

Those powers allow law enforcement to access significant amounts of data as part of their investigative powers. They could be supported with tools such as e-evidence that would allow law enforcement easier and faster access to the data that is already available, under control of the judiciary.

Furthermore, law enforcement should focus on exercising wholly the powers they already have: in some jurisdictions they may have been granted with some or even all of the powers listed above, but have not yet started to exercise them practically. In numerous cases, investigations could have been successful if only the capability of interpreting the already-existing data was improved.

4. Conclusions and recommendations

The Article 29 Working Party considers that:

- The availability of strong and trusted encryption is a necessity in the modern digital world. Such technologies contribute in an irreplaceable way to our privacy and to the secure and safe functioning of our societies.
- Encryption must remain standardized, strong and efficient, which would no longer be the case if providers were compelled to include backdoors or provide master keys. Whatever the technical solution, it can never be safe to compel encryption providers to include master keys and backdoors in their software.
- Law enforcement agencies already have access to vast quantities of data via their existing powers. Such access must remain proportionate and targeted. They should focus on improving their capabilities to interpret those data to investigate and prosecute criminals.

On behalf of the Article 29 Data Protection Working Party,

Andrea Jelinek

ARTICLE 29 Data Protection Working Party