20 May 2016

On lawful criminal investigation that respects 21st Century data protection. Europol and ENISA Joint Statement.

1 The communication society

The desire to preserve the secrecy and integrity of a document is as old as written communication, and is deeply inscribed in our modern legislation, touching basic rights such as freedom of expression and the right to privacy. With the move to the information society and the automation of data processing, this need is becoming ever more important. Moreover, these issues go beyond individual's rights: in a society that is ever more depending on the correct functioning of electronic communication services, technical protection of these services is mandatory, since otherwise criminals will abuse vulnerable services. From a technical standpoint, both confidentiality and integrity may be fulfilled by the same cryptographic mechanisms. However, while secure communication services have many legitimate purposes, they may also be used to plan and conduct criminal activities. Hence, law enforcement services need tools to investigate cybercrimes as well as cyber-facilitated forms of crimes.

2 The limits of privacy

An individual's rights need to be evaluated carefully in relation to the individual rights of others to find a balance between the individual interests of the persons concerned. Thus, in the face of serious crimes, law enforcement may lawfully intrude privacy or break into security mechanisms of electronic communication systems. Legislation must explicitly stipulate the conditions under which law enforcement can operate. Here, we want to stress the importance of ***proportionality*** for the use of intrusive investigative tools. This requires that the intrusive effect of the investigative measure is proportionate to the crime that was committed. It also requires the selection of the least intrusive measure to achieve the investigative objective. The legislation should include the provision of appropriate supervision to ensure that intrusive measures are used in accordance with these principles.

Intercepting an encrypted communication or breaking into a digital service might be considered as proportional with respect to an individual suspect, but breaking the cryptographic mechanisms might cause collateral damage. The focus should be on getting access to the communication or information; not on breaking the protection mechanism. The good news is that the information needs to be unencrypted at some point to be useful to the criminals. This creates opportunities for alternatives such as undercover operations, infiltration into criminal groups, and getting access to the communication devices beyond the point of encryption, for instance by means of live forensics on seized devices or by lawful interception on those devices while still used by suspects. Moreover, forensic methods that make use of physical fingerprints of devices might not help to intercept the communication content itself, but might provide other important clues for the investigator. Even so, there are cases in which there are no such alternatives and access to the concealed content can only be gained by a form of decryption.

3 Considerations on decryption

While no practical encryption mechanism is perfect in its design and implementation, decryption appears to be less and less feasible for law enforcement purposes. This has led to proposals to introduce mandatory backdoors or key escrow to weaken encryption. While this 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. Moreover, criminals can easily circumvent such weakened mechanisms and make use of the existing knowledge on cryptography to develop (or buy) their own solutions without backdoors or key escrow.

The latest generation of encryption tools allow forward secrecy, meaning that the disclosure of a long-term private key does not allow the deciphering of messages from the past.

4 Resolving the encryption dilemma

Solutions that intentionally weaken technical protection mechanisms to support law enforcement will intrinsically weaken the protection against criminals as well, which makes an easy solution impossible. So far, we observe a continued arms race between cryptographers and crypto-analysts. In terms of practical breaks, cryptographers are currently miles ahead, which is good news for all the legitimate users who can benefit from the improving protection of their data. However, there is no doubt that malevolent parties use the same techniques to conceal their criminal activities and identities. For the investigation and disruption of crimes, it is important to use all possible and lawfully permitted means to get access to any relevant information, even if the suspect encrypted it.

To achieve this, it would be worthwhile to collect and share best practices to circumvent encryption already in use in some jurisdictions. Investigators would benefit from more explicit and ideally aligned regulation of the lawful online use of privacy-invasive investigative tools and the conditions under which they can be applied. Moreover, policy makers in consultation with the judiciary could further contribute by issuing clear policy guidance on the proportionality of the online use of such privacy-invasive investigative tools.

When circumvention is not possible yet access to encrypted information is imperative for security and justice, then feasible solutions to decryption without weakening the protective mechanisms must be offered, both in legislation and through continuous technical evolution. For the latter, the fostering of close cooperation with industry partners, as well as the research community with expertise in crypto-analyses for the breaking of encryption where lawfully indicated, is strongly advised. We are convinced that a solution that strikes a sensible and workable balance between individual rights and protection of EU citizen's security interests can be found. In this respect, the deployment of European R&D instruments may drive this collaboration while at the same time EU Agencies can work closely together in establishing best practices.

This Joint Statement is presented as a contribution from ENISA and Europol to the on-going debate on privacy and encryption. It is based on the practical experiences and perspectives of the two organisations and is neither intended as being the formal position of the EU Institutions on this subject, nor as having any prejudice to that.