WE ARE SHAPING THE INTERNET.
YESTERDAY.TODAY.BEYOND TOMORROW.

eco

Background Paper on the Encryption Debate

Berlin, 10 July 2019

Encryption is a central component of IT security. Modern electronic communication services make use of them. For connecting to websites, it is now the predominant standard (https). Important Internet data is stored in encrypted form in clouds. In an age in which more and more devices and services are operated digitally, in which critical processes are increasingly being handled digitally, and in which these devices, services, and processes are interconnected via the Internet, the security of these services, devices, and processes is becoming a crucial issue. As the importance of IT security increases, so too does the importance of encryption. Awareness concerning secure services is also rising amongst users and consumers, as is the desire to be able to communicate with one another in confidence. This, too, is driving the propogation of encrypted communication, especially in messenger services. As a result, the Internet industry is relying increasingly on encryption in many areas. It is a central building block for trust in digital services.

At the same time, there is a growing interest on the part of governments and investigating authorities in having access to or in being able to monitor data and processes on the Internet. Through legislation and regulatory intervention in networks, services, user options, and in the technology itself, they are seeking for a variety of reasons to promote their access and monitoring capabilities. This is problematic. Because even if the underlying motivations driving these efforts may differ, they all create the same fundamental problems. With every weakening of IT security on the Internet, the increase in public security which is ostensibly being strived for actually becomes a threat to society through cyber crime, industrial espionage, and cyber war.

The debate on encryption comprises of a constant stream of discussion on the following measures for limiting and weakening encryption. These in turn are undermining confidence in the security and integrity of digital services and applications.

- **Specifications for the level of encryption:**

An incessant demand is being made for governments and authorities to be able to “crack encryption”. To realize this demand, the implication is that strong encryption should no longer exist. The specifications would allow for a regulatory intervention, which could undermine associated sophisticated security solutions and rule out the possibility of increasing the security level of products offered on the market.

A further problem is that such weak encryption can be more easily cracked not only by the respective governments and authorities, but also by any other actor in command of the relevant skills. As such, central specifications for the level of encryption are detrimental to encryption and to IT security. In this context, it should

also be made clear that centrally imposed security levels which generally preclude exemptions and at most tolerate them as derogations could give rise to similar outcomes and should therefore be avoided.

- **Key production**

Encryption is now established in the field of electronic communications services. Almost all of these services use different forms of encryption, which is frequently dynamic and, as end-to-end encryption, cannot be easily broken.

Against this background, a number of actors are calling for providers of electronic communications services to be able to decrypt their users' messages themselves, at least on request, and to make the content available to investigating authorities. It would be similarly problematic if parts of the key had to be handed over so that the decryption of messages could be faster or easier. In such a case, with a sufficient number of keys passed on, the mathematical procedure behind them could be recognized and the encryption for all messages could be removed. Moreover, in both cases, an encryption method would have to be chosen which would enable the service operator to decrypt the messages of its users. Particularly secure encryption methods, such as those used in OTT messenger services, would thus no longer be possible.

- **Backdoors / Transfer interfaces**

A demand doing the rounds is that operators of services must provide an interface for extracting and reading inventory data and content. This would also present the problem that end-to-end encryption would not be possible and that the encryption level would thereby be weakened.

A further problem with this measure would be that such a transfer interface could also offer a gateway for hackers trying to intercept communications and use them for their own purposes.

Conclusion:

Measures that weaken encryption ultimately also weaken the security and integrity of digital systems and services. In an interconnected world, they offer a springboard for damaging and imperiling other systems and networks, the privacy of users, and economic activity. They undermine confidence in these services, in digital technologies and aside from this in business, the state, and society. Governments and international organizations around the world should work to ensure that regulatory weakening of encryption is not imposed. Users must be given the opportunity to use encrypted services and applications without fear of sanctions.

Encryption must be proactively promoted and its use and propagation supported by research projects and information services. Encryption methods must not be regulated in such a way as to lower or suspend security levels. Known vulnerabilities

and security gaps must be disclosed to operators of services or security solutions so that remedies can be found.

About eco: With over 1,100 member companies, eco is the largest Internet industry association in Europe. Since 1995 eco has been instrumental in shaping the Internet, fostering new technologies, forming framework conditions, and representing the interests of members in politics and international committees. eco's key topics are the reliability and strengthening of digital infrastructure, IT security, and trust, ethics, and self-regulation. That is why eco advocates for a free, technologically-neutral, and high-performance Internet.