BRUSSELS
PRIVACY
HUB
Vrije Universiteit Brussel

# 38th Annual Conference of Data Protection and Privacy Commissioners
# Marrakech, Morocco
# Closed Session: Encryption and the Rule of Law: An International Conversation
# 17 October, 2016

**Summary of remarks by Prof. Christopher Kuner**
**Co-Director, Brussels Privacy Hub, VUB Brussel, Belgium**

This short paper encapsulates the remarks on encryption that I made at the closed session. As this is a summary of my speaking notes, it is brief and does not go into detail.

## Encryption in historical perspective

The historical dimension of the encryption debate is often neglected. There are precedents to the current tensions between privacy and law enforcement interests that are illuminating with regard to present-day problems, since the same tensions with regard to encryption that we are grappling with today have occurred throughout history. The historical record demonstrates that we can never regard the protection of privacy on the Internet as a problem that has been "solved", and that the lessons from the debate on the regulation of encryption will have to be re-learned on a continuing basis.

An example is provided by the so-called "crypto wars" of the 1990s, in which the US and some other countries attempted to mandate the use of "key escrow". This would have required users of encryption technologies to deposit hardware and software keys used to encrypt communications on the Internet with governments, or to build "back doors" into them so that governments could gain access to encrypted data.

I experienced the crypto wars as an opponent of key escrow while working as a lawyer in Germany in the 1990s. The debate in that country and elsewhere was often heated, with law enforcement agencies arguing that key escrow was necessary to maintain their existing capabilities with regard to communications on the Internet. On the other side of the debate were privacy advocates and many (but not all) multinational companies, who opposed these plans.

In the late 1990s, the US government seemed to drop its key escrow campaign, as it became clear that a number of foreign governments would not support it, and as encryption companies based outside the US began to spring up. Thus, it may have seemed at the time that opponents of key escrow had won the crypto wars.

The Snowden revelations have shown how naïve we were. It is true that governments in western democracies have not passed legislation obliging users of encryption technologies to deposit encryption keys with government agencies. But we have learned that law enforcement agencies are apparently accessing Internet communications on a massive scale notwithstanding the lack of the kind of key escrow framework that some governments lobbied for.

It thus seems that law enforcement agencies and governments actually won the crypto wars, but did it so cleverly that we did not realize it. The fading of efforts to push mandatory key escrow was not an expression of defeat, but a shift in strategy prompted by a realization that governments could get the massive access to electronic communications data that they wanted without the public debate that the crypto wars produced.

Another historical example occurred much longer ago. In the period 1890-1914 global trade doubled and there was the greatest international migration in history, which show the parallels with the present day. During that time there was also a significant level of political violence from anarchists and radical socialists, leading to the assassinations of many high-ranking political figures such as the US president, the Tsar of Russia, the French President, the Prime Minister of Spain, and the Empress of Austria, and the deaths of numerous civilians. The mood of that age is captured in Dostoyevsky's great novel *Demons* (also known as *The Devils*), which illuminates the phenomenon of terrorism is in a way that remains highly relevant today.

Disputes about the use of encryption by terrorists also occurred in those years. Taking just the example of Tsarist Russia, there was a technological arms race between revolutionaries and the secret police concerning the use of encryption, as well as widespread surveillance of the postal system, which included the use of so-called "black chambers" in which all foreign mail and a selection of domestic mail was read by the security services.

The cycle of anarchist and radical socialist violence in the late 1890s and early 1900s did not end because of a resolution of the encryption dilemma, but because of social factors such as increased economic prosperity, social stability, and migration controls, as well as the outset of World War I. Similarly, the current encryption debates are not susceptible to a simple "solution", but will have to be resolved through social developments that will likely take a good deal of time to play out.

## The role of encryption in data protection law

Encryption plays an important role in data protection law. Security of data processing is a major principle of data protection law, and the increasing importance of data security is reflected in changes that have been made and are being made to the law.

For example, the new European Union General Data Protection Regulation (GDPR), which will apply from 25 May 2018. The GDPR specifically mentions encryption several times as a way to mitigate the risks of data processing. This can be seen in Recital 83, which mentions encryption as a way to mitigate data security risks; Article 6(4)(e), which lists encryption as a type of appropriate safeguard to be taken into consideration when the data controller has to ascertain whether processing for another purpose is compatible with the purpose for which the personal data are initially collected; Article 32(1)(a)), which includes encryption as a factor to be taken into account when determining the appropriate level of data security; and Article 34(3)(a), which exempts data controllers from communicating data breaches to data subjects in cases where encryption has been used to make the data unintelligible to unauthorized persons.

Encryption will become increasingly important in data protection law, as the law moves more towards a risk management approach, and as data security risks continue to increase. I suspect that in the coming years, encrypting data will become routine for data controllers and service providers, and that even when encryption is not explicitly required by law, it will become so ingrained as a best practice that regulators and courts will penalize data controllers and data processors who do not use it.

**The legality of restrictions on encryption**

The conflict between privacy and law enforcement interests have caused a number of restrictions on encryption to be proposed, ranging from requiring that weaknesses or ”backdoors” be built into encryption technologies; requiring users to deposit keys with law enforcement authorities; restricting the sale and distribution of encryption products; requiring companies that produce encrypted devices or software to decrypt messages that have been encrypted; and others.

Such restrictions must be evaluated under international human rights law, which provides principles to judge their legality. Particularly relevant here are Article 17 of the International Covenant on Civil and Political Rights, and Article 12 of the Universal Declaration of Human Rights, which together provide the basis for the right to privacy in international law.

The right to privacy can only be limited under strict conditions. Because encryption is used to protect privacy rights, restriction of it should be judged under human rights law requiring that the principles of legality, necessity, and proportionality be respected. To describe these principles briefly and superficially, legality means that restrictions on encryption may be imposed only on the basis of a law; necessity requires that restrictions may be enacted only for legitimate purposes and must actually yield benefits toward such a purpose; and proportionality requires that the least intrusive measure that might achieve the desired result be chosen. This suggests that indiscriminate, non-targeted access to encrypted communications, or broad restrictions on the use of encryption, are highly questionable under human rights law.

The debate surrounding encryption has been largely political, and is often not conducted with the above-mentioned considerations of international human rights law in mind. The law defines what kinds of restrictions on encryption are permissible and which are not, but the scope and substance of the law is determined by the political process. Thus, in the end the balance between privacy and law enforcement interests will depend on agreement being reached at the political level as to what sort of society we want to live in.