Encryption protects security and privacy

Keynote speech at Assemblée nationale française

Paris, 21 November 2016

Giovanni Buttarelli

Monsieur le Président,

Mesdames, messieurs les ministres,

Madame, Messieurs les présidents de groupe,

Mesdames, messieurs les députés.

C'est un vrai honneur pour moi de prendre la parole devant cette illustre assemblée. Je propose de vous adresser quelques mots à ce sujet en anglais, avec votre aimable autorisation, Monsieur le Président..

Today's debate comes at a crucial moment in time. We all saw recently a common letter of the Ministers of the Interior of France and Germany, Messrs Cazeneuve and De Maiziere, expressing concern about the need to access communications data.

In a couple of months, the European Commission will disclose its proposal to review ePrivacy rules and reveal its approach to protection the fundamental right to privacy, established by Article 7 of the EU Charter or Fundamental Rights.

One of the questions in the debate on this instrument will be the relationship between the fundamental right to privacy and the powers and tools available to law enforcement and security agencies.

We have been through this debate already in the past, and we have received a response from the EU's highest court when it annulled the data retention directive. It found that the EU legislator had not properly assessed the necessity and proportionality of the data retention measures it obliged communications providers to implement.

As the ePrivacy Directive is defining the limits to interception and retention, its reform will be influenced by the new debate over communications privacy and the fight against terrorism.

Now, I am a privacy regulator, but I am also a judge with years of experience handling sensitive cases concerning the intelligence, mafia and organised crime. I helped draw up anti-mafia legislation in the wake of the murders of judges Falcone and Borsellino. My EU institution will soon become responsible for overseeing the compliance of Europol with data processing rules.

As the head of an EU institution, I of course work in Belgium, a small country.

Tomorrow, the 22nd November, it will have been eight months exactly since we experienced the country's worst ever terrorist act, 32 people were senselessly murdered.

It was the latest in an arc of mayhem beginning here in Paris with the Charlie Hebdo attacks in January 2015, through the massacres in and around Paris in November, before eventually moving to Brussels itself, the city where the cell of radicalised young men had formed and grown.

I understand as well as anyone that security and law enforcement bodies require the appropriate means to fight crime, including on the Internet. However, for any new measure, there is a need to assess beforehand the necessity and proportionality of the measure envisaged and to provide substantiated evidence of the necessity of those measures.

Where is the debate in Europe right now?

First of all, let's remember that European law – the European Convention on Human Rights, the Charter of Fundamental Rights of the European Union, even the Lisbon Treaty – is the result of an attempt to exorcise the ghosts of totalitarian government in most of the continent in the 20th century.

In human rights law, everything returns to the individual. The notion of 'security' for example is only ever understood by the European Court of Human Rights as personal liberty.

Privacy, including confidentiality of communications, is a fundamental enabler for a free and democratic society. Without privacy, fundamental rights cannot be guaranteed and trust will disappear. Free speech, the right to assembly and many other freedoms will be in danger when all communications are feared to be subject to surveillance.

When we assess the necessity and proportionality of measures giving access to our communications to police and security forces, we must carefully weigh the arguments.

We have launched a discussion on this process by asking for contributions on a discussion paper on a necessity toolkit this summer.

When we consider the privacy of communications, and measures to make it secure against interference, we must also consider its importance for the functioning of our economy and society.

Information security as security of data, systems and networks is crucial for the integrity of transactions and development of the Digital Single Market, Smart Grids and the Internet of Things to name just a few. Weakened data security for the sake of allowing more pervasive surveillance would destroy trust and undermine not only the EU single market, but the electronic business as a whole.

Encryption has grown into a critical tool to protect confidentiality of communications. Its use has increased after the revelations about efforts by public and private organisations and governments to gain access to our communications.

If we create backdoors in our devices or in our encryption schemas, criminals and terrorist, the supposed targets of these measures, will abuse the reduced security of our devices or encryption for their purposes. Reducing the security of our devices will endanger our information, our personal data and our fundamental rights.

Just imagine if the state instructed all architects and construction companies to weaken, in a secret way, one of the points of entry in every private residence.

Would that be acceptable to society at large?

Of course not. Because we know that it would be an open invitation to burglars to break into our homes.

Making encryption breakable for state authorities can only be achieved in two ways:

> Either all encryption algorithms used by citizens and businesses must be weakened intentionally, or
>
> All businesses and citizens are forced to hand over their secret encryption keys to the state (*key escrow*).

On a basis of available evidence, we assume that neither of these approaches can work in practice:

> To ensure that only weak encryption is used, all software running on computers, laptops, tablets, smartphones, etc. would need to be controlled. The only possible way would be to criminalize the possession and use of strong encryption software.
>
> A database or system keeping the secret keys for all encrypted communications would be a critical risk for national security. It would be an incredibly valuable target for criminals, and carry a high risk of abuse by national or foreign intelligence or disloyal staff.

Furthermore, the measures would not have the intended effect. Law-abiding citizens and businesses would follow the rules and suffer from reduced trust and security, while criminals would use strong security and encryption.

In summary, weakened encryption would enable mass surveillance of loyal citizens; effectiveness, necessity and proportionality of which are not proven.

For targeted surveillance, technical measures exist that can circumvent also strong cryptography but do not affect society and economy as a whole.

To pass the test of necessity and proportionality, measures must also be **effective**. This means that they have to work and to contribute to achieving the intended objective. Measures that do not work cannot be proportionate and necessary.

We closely follow the debate and we understand the need for law enforcement bodies to act. However, we cannot see convincing evidence that any restrictions on encryption are effective enough to justify the interference with fundamental rights and freedoms that they would cause.

In fact, it may now be time - as I said in my address to a conference at Europol in May this year - to consider establishing a right to encrypt, in addition to any moves to reinforce law enforcement capabilities.

To guarantee our fundamental rights users should be allowed to use end-to-end encryption (without *back-doors*) to protect their communications. Decryption, reverse engineering or monitoring of communications protected by encryption should be, in principle, prohibited.

This is what I have recommended to the EU legislator in my opinion on the review of the ePrivacy Directive.

Ladies and gentlemen, we all understand that legislators feel the need to act in reaction to events of great public concern. My recommendation is to take their responsibility for fundamental rights and the very fabric of our democracies seriously, and not to use unjustified restriction of fundamental rights lightly, because it seems and easy and low-cost measure.

This is not the case, there is a high political prize and there is strong indication that we also would pay an economic prize when we break the tools that enable our digital economy.

Thank you for your attention.