EDPS

EUROPEAN DATA PROTECTION SUPERVISOR

Cybersecurity under the next president: A Symposium with cybersecurity industry leaders

Closing speech at Coalition for Cybersecurity and Law Symposium

San Francisco, 15 November 2016

Giovanni Buttarelli

I'd like to thank Ari and the Coalition for Cybersecurity Policy and Law for their kind invitation to be with you this afternoon.

It has been an education and a privilege to hear such expert and varied opinions about the situation we find ourselves in.

I was asked to provide a European perspective;

But let me tell you that the European perspective on cybersecurity is not much different from the one here in the US.

Our political situation is also in flux. Following the elections this month in Lithuania and Bulgaria, between now and end 2017, there will be general elections in a further seven European Union member states, including France, Germany, Netherlands and Luxembourg – four of the six founding members of the EU.

This is in addition to the uncertainty around the constitutional referendum in my home country.

And I haven't even mentioned Brexit yet!

And we also are more vulnerable than ever to cyberattacks. This applies equally to European Union institutions, such as my own – there was a well-documented attack on the systems of the European Parliament and Commission back in 2011.

The first panel today analysed the notion of vulnerability.

It is an inescapable fact that vulnerability is intrinsic to the digital society.

This is recognised in a new law in the EU, Directive 2016/1148 on security of network and information systems.

The directive was published in July this year and must be incorporated into national laws by 9 May 2018.

Its premise, as set out in the preamble to the directive, is the growing frequency and impact of security incidents.

With the directive, the EU is trying to establish a new generation of common, higher security for networks, services, data and information systems.

The preamble also lists what might be described as the EU's 'vulnerable entities':

- economic activities
- user confidence
- the economy of the Union

- cross border movement of goods, services and people, in other words, the smooth functioning of the internal market.

This 'NIS Directive' has a number of essential building blocs

- the identification of national strategies
- identifying operators of 'essential services'
- highlighting which significant disruptive effects are at stake and the role of Computer Security Incident Report Teams

In addition to the NIS Directive there are some important trends in security breach notification.

The other more high-profile legislative moment for the EU in this area was the adoption of the 2016 General Data Protection Regulation.

We have heard that today the Department for Homeland Security has published its 'Strategic Principles for the Security of the Internet of Things' and that the first of these principles is to 'Incorporate Security at the Design Phase'.

This is an echo of the new requirement in the EU data protection regulation for developers to integrate data protection by design and by default.

Since 2009, under the EU ePrivacy Directive, there has been an obligation on all providers of publicly available electronic communications services to notify security breaches.

The new data protection regulation extends this obligation to all persons responsible for processing personal information. Data security is now a clear legal obligation for any company targeting its services at the EU or processing personal information concerning people in the EU.

If there is a failure to comply, the regulation provides for severe sanctions of up to 10m EUR or 2% of total global annual turnover.

One of the questions throughout this discussion has been how vulnerability should be assessed.

The EU data protection regulation sets out a number of tools: for example, data protection impact assessments for all operations likely to pose a risk to individuals.

But meeting cybersecurity challenges is not simply about the law.

We have heard about the importance of information sharing at an international level and between the public and private sectors.

This is the goal of the Cybercrime Centre, set up in Europol in 2013, and the implementation of the Council of Europe's 2001 Budapest Convention.

In considering the balance of interests between companies, governments and individual consumers and citizens, encryption has become a pivotal question.

We also know that embedding surveillance in communications infrastructure creates long term security risks - we have been discussing this in the digital age since Professor Susan Landau's prescient work in the early 2000s.

Recently in a joint letter the Ministers of the Interior of France and Germany expressed grave 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 right to privacy: a fundamental right which has a constitutional status for the European Union.

We know from the case of the data retention directive that EU law has to pass the tests of necessity and proportionality.

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.

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.

Deliberate weakening of encryption algorithms used by citizens and businesses is not the answer – this is recognised in a joint statement from Europol and the European Network and Information Security Agency.

Forcing all businesses and citizens to hand over secret encryption keys to the state isn't the answer either.

A database or system keeping the secret keys for all encrypted communications would be a critical risk for national security.

It would be an early Christmas present for criminals and hostile intelligence services, while diminishing the confidence of individuals in networks and information systems.

We actually need targeted surveillance which minimise adverse impacts on society and economy.

Reinforcement of law enforcement capabilities may need to be accompanied by a right to encrypt.

A right of citizens to use end-to-end encryption (without back-doors) to protect their communications.

But we need to look beyond current capabilities, to quantum and post quantum cryptography.

We need to calculate, as Michele Mosca has argued,[1] whether the 'security shelf life' of current applications and the time needed to deploy quantum-safe tools will be greater

[1] Cybersecurity in an era with quantum computers: will we be ready, Michele Mosca, 2015.

or lesser than how long it takes for a quantum computer to breaks our current public-key cryptography tools.

So in conclusion:

Europe faces the same threat and challenges as the US.

Our legal system is different, but it is premised on the same values of democracy and freedom and the rule of law.

We need to find the right mix of sustainable laws and obligations, effective enforcement, transparency and cooperation.

And we need to place the interests of the ordinary individual at the centre of the encryption debate. We need to avoid measures which address short term needs by which create long term vulnerabilities for both individuals and national security.

I hope we can organise a similar event in the EU to which you will all be warmly invited.

There are difficult days ahead, so the need to work together has never been more clear.

Thank you for your attention and thanks for the excellent symposium.