Speech on Key Challenges for Privacy in the Digital Age

Speech to Europol/ EIPA conference on Privacy in the Digital Age of Encryption and Anonymity Online

The Hague, 19 May 2016

Giovanni Buttarelli

Ladies and gentlemen,

I'm really delighted to be here at this event today.

A big thank you to Rob Wainwright for the invitation.

And a big thank you also to the team Europol and to Marga Pröhl and EIPA for organising the conference.

As we have just heard during the welcome messages from Rob, Marga and Udo Helmbrecht, this conference juxtaposes three red hot topics for public policy: privacy, encryption and anonymity in the digital age.

Furthermore, I understand that this is the first public event which Europol has held on the specific subject of privacy. It is an impressive initiative by the EU's law enforcing agency to lead by example on safeguarding fundamental rights, and I commend the Director for doing this.

Allow me to spend the next 10 minutes to share some thoughts on important legal developments in the EU, on the broader question of privacy and surveillance, and the specific topic of encryption.

My mantra since taking office as EDPS has been the following: data protection in the EU needs to go digital: digital data protection which is effective in practice, dynamic and user-friendly, with the emphasis not on procedures but on real safeguards for the individual.

This is more than a slogan.

It means understanding better what is happening in cyberspace - the global and ubiquitous and instantaneous flows of personal data, what that means for us as individuals, and what that means for us as regulators and indeed law enforcement authorities.

So this conference is about taking privacy and data protection into the new fast-evolving digital world.

Europe has taken a massive step in the right direction this month.

The final adoption of the General Data Protection Regulation and of the Directive for data protection in the police and judicial sector are major developments. These are the first of a new generation of rules for the Web 2.0, for the fourth industrial revolution, or whatever you want to call the new era of hyperconnectivity. They ensure that Europe remains in the global vanguard for data protection and privacy.

And now, just a couple of weeks later, we have adoption of the Europol Regulation.

This Regulation is important for many reasons. Of course it has a big impact on my institution, which will become responsible, in 2017, for the supervision of compliance of personal data processing, in cooperation with national supervisory authorities.

Data protection has always been part of the Europol's DNA, ever since the 1995 Europol Convention.

1995 was also the year of the old Data Protection Directive. Now in 2016 both frameworks have been reformed. You might say that Europol's evolution has in fact been in lockstep with the EU's Data Protection framework.

Later today I will be meeting colleagues from the Europol Joint Supervisory Body and with the Director to continue initial discussions on the transition, to ensure that we are fully ready from day one.

There is no need to impress on me the importance and sensitivity of the work which Europol does.

My institution has extensive experience of the supervision of EU-wide large scale information sharing, including the Schengen Information System, the Visa Information System, Eurodac and the Customs Information System.

Speaking personally as a member of the Italian judiciary, I have direct experience of investigation into organised crime and antimafia prosecutions.

The crucial factors in all effective and successful investigations are willing cooperation between agencies, having access to the right information, and using that information in a smart way.

EU data protection law is not an obstacle to these factors. Rather it enables responsible and proportionate practices.

They used to say that if there is a new problem, the solution was to set up a new agency.

Nowadays, it seems that the solution is to set up a new database.

But we know that life is not so simple.

Databases do not catch criminals or prevent terrorist attacks.

But smart law enforcement officers do.

Of course law enforcement authorities need to do everything possible to fulfil their public function of ensuring law and order and justice for victims of crime and terrorism.

The EU's Counter Terrorism Coordinator recently told the JHA Council that there are still 'significant gaps with regard to feeding Europol' with information necessary on foreign terrorist fighters. This is an urgent problem because of the need for Europol to help match criminality and terrorist activity. It is likely that most of the Paris and Brussels attacker were known to the local police as criminals, jihadis or some foreign fighters, and that information on them was included in the relevant EU databases.

The problem was not lack of information. It was lack of sharing and inadequate analysis.

Last month there were two separate cases in Germany and Italy, where the countries' highest judges considered the essential legal concepts of necessity and proportionality.

The German Federal Constitutional Court ruled on the proportionality of Federal Criminal Police Office covert surveillance measures like use of tracking devices in order to protect against threats from international terrorism.

The Court said that intruding into the private sphere affects human dignity, while effective information gathering is needed for fighting terrorism and for protecting fundamental rights, and that these constitutional rights ranked equally.

But it found that the provisions of the law were too broad - and lacked privacy safeguards, transparency to parliament and public and individual legal protection and judicial review.

So, according to the Court, it was disproportionate to use wiretap for more than just the most serious offences; and there were limits on the interference with the private spheres of individuals who are not suspected of terrorist activities. And it was disproportionate also to transfer personal data to third countries where there were no guarantees of protection of the fundamental rights of the individuals in question.

Meanwhile, also in April this year, the Italian Court of Cassation said that evidence acquired through Trojan Horses installed on electronic equipment could only be admissible, under current national law, in the most serious cases of crime - anti mafia, organised crime and terrorism. The judges recognised that even if it was possible to apply such measures for other purposes or crime in general, this would go beyond what was necessary and proportionate and that there would be serious privacy implications.

In the EU, the ultimate arbiter is the European Court of Justice in Luxembourg. It is the Court, not the European Parliament or DPAs, that must be convinced that a measure which interferes with individual rights is justified.

There is now plenty of case law, in Luxembourg and from the European Court of Human Rights, on the limits of surveillance and other measures meant to tackle crime and terrorism.

The most famous is the Data Retention Directive case. This year we await rulings on the legality of the EU Canada PNR agreement and national data retention laws.

We can expect the Court to scrutinise these measures on the basis of whether the provisions are precise and foreseeable in their effects, of whether they are targeted

according to clear criteria, instead of authorising indiscriminate collection of personal information, and of whether they contain safeguards in terms of data security and independent oversight of compliance.

The same will apply in the event of final agreement on the EU-US Privacy Shield agreement on commercial transfers of data, where legal challenges can be expected whatever the outcome.

That is why, in the next few days we will soon publish a toolkit for EU policy makers and law makers to help them with the delicate but essential task of assessing necessity of a measure which interferes with fundamental rights to privacy and to data protection.

But Europol and the many other law enforcement specialists assembled here know well that every day there are big questions, big judgment calls.

Over the next two days we will be talking about encryption and anonymity. These two words have entered the lexicon of privacy, because they are about how ordinary people are seeking to preserve their own private sphere online, just like they have always sought to preserve their private sphere offline.

There has been a heated debate about backdoors.

Lawful intercept means seeking the approval from a judge to record the communications of a target. They then must destroy the data when no longer needed.

A backdoor could be fundamentally different from the traditional wiretap. Much more so than our homes, our mobile devices now contain revealing and sensitive data on almost every aspect of our lives, private and professional.

A Trojan Horse or built-in vulnerability in all smart phones, tablets and PCs would allow collection and retention of personal information on a much greater scale than ever before. It would set a precedent for the emerging Internet of Things where a whole range of everyday devices and objects will be connected.

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.

I know that ENISA and Europol have been discussing this issue. And I am pleased that we are on the same page on this question - that 'backdoors' are not the solution to cybersecurity, they would be a new and dangerous part of the problem.

What we need instead is to reinforce the global infrastructure, not to weaken it, to ensure that not only citizens but governments also are secure against attacks.

In fact, it may now be time - as I said in my address last month to New York University Center on Law and Security - to consider establishing a right to encrypt, in addition to any moves to reinforce law enforcement capabilities.

Ladies and gentlemen,

The FBI-Apple argument in the wake of San Bernardino is just an early skirmish in a long battle.

A broad and informed public debate is now needed, just as President Obama himself has said.

So I welcome the debate which Europol is facilitating today and tomorrow.

I would like to leave you with one key consideration. Is the question really one of privacy versus security, or is it rather one of overall security versus decryption?

What is clear is that the debate needs to be multi-disciplinary, on how to ensure access by law enforcement bodies to private content only occurs where lawful, transparent, selective and proportionate.

Thank you for listening, and I wish you a very fruitful and stimulating conference.