Counterterrorism and Data Privacy: A European Perspective

Speech to the symposium on Governing Intelligence: Transnational Approaches to Oversight and Security

Hosted by the Center on Law and Security and the Woodrow Wilson International Center for Scholars

New York, 21 April 2016

Giovanni Buttarelli

Let me first thank Dean Trevor Morrison, Zach Goldman - and everyone at the NYU Center on Law and Security and the Woodrow Wilson International Center for Scholars - for holding this event and for the kind invitation for me to join in the discussion.

This is such an important topic.

The discussion today comes just after the Council of the EU adopted the EU-Passenger Name Records Directive - a controversial measure. And it also comes a day after the German Federal Constitutional Court ruled on the proportionality of surveillance and anti-terrorism measures - a ground breaking judgment

Vigorous and open discussion is a hallmark of democracy in this country.

You are tackling face-on an area which is too often in the shadows, too far away from public discourse – in Europe as well as other places.

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.

I understand as well as anyone the importance for law enforcement of quick access to all relevant information

I've just come from Harvard where I gave a speech refuting the assertion that 'privacy is dead'. In fact, you are probably familiar with statement by an NSA director following the WikiLeaks disclosures in 2010 that "There's no such thing as 'secure' anymore."[1]

Obviously privacy and security have always existed, and are not likely to disappear in the near future.

People try to eliminate all risks, and governments try to promise that they can deliver this.

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

Tomorrow, the 22nd April, it will have been once month exactly since we experienced our own 9/11.

In the country's worst ever terrorist act, 32 people were senselessly murdered.

It was the latest in an arc of mayhem beginning 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.

Just like the US in 2001, Belgium and the EU are realising that the problem is joining the dots.

The people involved were known to the different authorities. The problem was not the lack of information. The problem was that appropriate action was not taken on the basis of that information.

In the strategy for my mandate as EDPS, I have called for a more mature debate on national security and privacy.

We need to look at the actual needs of our intelligence agencies. What works and what doesn't work. And what is the cost in terms of individual rights and the freedom of the vast majority of citizens who have not committed any crime and have no intention of doing so.

That was, in essence, my first message in the EDPS Opinion which we published in February on the EU-US umbrella agreement on law enforcement information sharing: we need this agreement; fighting crime is too important to be left in legal limbo.

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.[2]

[1] Quote attributed to Debora Plunkett head of the NSA's Information Assurance Directorate in 2010; www.reuters.com/article/us-cyber-usa-nsa-idUSTRE6BF6BZ20101217 [accessed 20.4.2016.]

This helps explain why the case law of that court[3] has held that, if law enforcement access personal data, then it is a bigger interference with individual rights compared with access by private parties.

And the UN Special Rapporteur on the promotion of human rights and fundamental freedoms in his 2014 report effectively echoed the notion in EU law of the essence of a right to privacy being compromised and undermined when correspondence is monitored on massive scale.

So the law must be precise and allow people to protect their data against abuse.[4]

However, there is no definition of the concepts of 'national security', 'internal security' and 'public security', terms which occur variously in the EU's Lisbon Treaty.

I spent a lot of time discussing with my interlocutors in the Federal Administration and in the EU the meaning of 'targeted' versus 'untargeted' or 'bulk'. Presidential Policy Directive 28 attempts a definition of 'bulk', but for many people it is not fully satisfactory because we don't know what is meant by a 'discriminant' - how broad a search criterion it could be.

There have been various attempts in the EU countries and in the US have to define 'targeted' and 'bulk' but it has never made it into law.

Similarly there is no clear common understanding or legal definition of the meaning of SIGINT, though again venerable institutions like the Venice Commission have tried.

When the CJEU struck down the EU Data Retention Directive, it reiterate the concerns of European Court of Human Rights in a previous case which found against the indefinite storage of personal information, blanket and indiscriminate, collection with no distinction between types of sentences and so on. The CJEU found data retention to be a disproportionate violation of the right to privacy.[5]

'Mass indiscriminate surveillance is inherently disproportionate and constitutes an unwarranted interference with the rights guaranteed by articles 7 and 8 of the Charter,' according to the AG Opinion, in *Schrems*, September 2015.

The European Court of Human Rights has recently reiterated its condemnation of any indiscriminate potential to spy.[6] The Court seemed particularly sceptical about broadly determined definitions in the context of 'national, military, economic or ecological security' which confer 'almost unlimited degree of discretion' – notwithstanding the requirement for judicial authorisation.

---

[2] Similarly, in its 1990 landmark ruling, Human Rights Committee, in *Delgado Paéz v Colombia*, treated article 9.1 of the ICCHR as an independent right with a corresponding state obligation to protect the individual against death and other serious threats.

[3] *Leander v. Sweden* judgment of 26 March 1987, Series A no.116; *Rotaru V. Romania. (Application No. 28341/95). Judgment. Strasbourg. 4 May 2000, Weber and Saravia v Germany Application No 54934/00, Admissibility, 29 June 2006*.

[4] *Liberty And Others V. The United Kingdom* (Application No. 58243/00) Judgment Strasbourg 1 July 2008*; Rotaru ; S And Marper V United Kingdom [2008] ECHR 1581*)

[5] Digital Rights Ireland and Seitlinger and others, Joined Cases C-293/12 and 594/12, 8 April 2014.

[6] *Roman Zakharov -v- Russia*; ECHR 4 Dec 2015. December 16, 2015. References: 47143/06, para 248; *Szabó And Vissy V. Hungary. 37138/14*, 12/01/2016.

The European Court of Human Rights has accepted that rights can be limited where justified.[7]

The EU's Fundamental Rights Agency with whom we work closely is carrying out, at the request of the European Parliament, research into the legal frameworks and oversight bodies governing surveillance activities in EU countries.

Among its findings were that oversight bodies consistently were denied access to relevant information, and no parliamentary committee had unrestricted access to intelligence information.

The FRA initial report was last November. It has found that only five of the 28 Member States have detailed conditions on use of targeted and untargeted surveillance.

Twelve EU data protection authorities have no competence at all over intelligence services.

The first step for trust and accountability is transparent and accessible legislation.

Even so, the CJEU consistently accepts the legitimacy of the objective of general interest of fighting international terrorism and serious crime.[8]

And Article 4.2 of the TEU clearly ring-fences national security as a competence for governments - 'the sole responsibility of each Member State'.

In Europe, by means of the specific legal provision of data retention, the courts are now exploring the boundaries of this competence: according to the CJEU, even measures derogating from EU law are subject to the Charter.[9]

Courts are one thing. The actual practice of states is another.

There is an intriguing circularity in the debate about human rights, technology, security and surveillance.

External accountability is essential, but people in the agencies must be themselves committed to democracy and human rights. In other words, there needs to be an ethical basis for the work which they do, which can command the confidence and respect of society and its elected representatives.

The key driver for modern computing was in fact spying, whether at Bletchley Park in the Second World War or in Silicon Valley in the Cold War.

According to a recent book by the BBC's security correspondent, the mini super computer which we all now carry around have, in effect, automated espionage: they collect and disseminate information about our private lives 24 hours a day.[10]

---

[7] *Klass and others v Federal Republic of Germany, European Court of Human Rights (Series A, NO 28) (1979-80) 2 EHRR 214, 6 September 1978*.

[8] *Case C–402/05 P and C–415/05, P. Kadi and Al Barakaat International Foundation v. Council and Commission [2008] ECR I–6351, case C-145/09 Land Baden-Wurttemberg v. Panagiotis Tsakouridis, 2010 ECR I-11979; Digital Rights Ireland*.

[9] *Case C-399/11, Stefano Melloni v Ministerio Fiscal, judgment of 26 February 2013; Case C-411/10 N. S. v Secretary of State for the Home Department et M. E. and Other, judgment of 21 December 2011*.

On Tuesday I met one of the inventors of the World Wide Web. His team at MIT are trying, in effect, to reverse engineer the internet, to return it back to the distributed, decentralised model which they had originally hoped would empower the individual, not enslave her.

The other big conflict is the so called crypto wars.

Intentional weakening of cryptography causes a lot more damage than the advantages which are asserted. There are constant and innumerable attacks by criminals on systems looking for weaknesses. And closing down private innovation in data security is unlikely to result in stronger systems

When I met on Tuesday at MIT authors of a report aiming to end the current 'crypto war', they said that in their view it was not a war between privacy and security, but rather about needs of law enforcement vs security of the entire system.

In fact we may have reached a moment where we need to establish a right to encrypt.

So we need a more sophisticated approach.

Frank La Rue, special rapporteur on promotion and protection of right to freedom of opinion and expression, made a very important point in his 2013 report. Many authorities from different states, in accessing personal data, are effectively claiming extra territorial effect for their national laws. And yet we have no global approach to regulation of these global data flows.

That is why this debate today is so vital.

Big data is offering opportunities not just for online behavioural advertising, but for anti-crime as well.

Santa Cruz CA in 2011 implemented predictive policing leading to a reported 27% reduction in burglaries[11]. In March 2016, the US National DNA Index had 12.3m offender profiles[12].

Bruce Schneier in *Data and Goliath* argued that 'in a sense, we're living in a unique time in history; many of our surveillance systems are still visible to us'.

The challenge is to keep it that way.

Thank you for listening.

---

[10] Gordon Corera, *Intercept: The Secret History of Computers and Spies.*

[11] Opinion of the European Group on Ethics in Science and New Technologies to the European Commission: Ethics of Security and Surveillance Technologies, Opinion No 28, 20.05.2015.

[12] FBI CODIS — NDIS Statistics http://www.fbi.gov/about-us/lab/biometric-analysis/codis/ndis-statistics [accessed 20.4.2016]