Vienna Parliamentary Forum on Intelligence-Security

Vienna Hofburg, 6 May 2015

Giovanni Buttarelli

European Data Protection Supervisor

First of all[1], may I thank Andreas Schieder, Chair of SPÖ Parliamentary Group, for the invitation to this Forum. It is an honour to be among such a distinguished gathering of parliamentarians from Europe and the United States.

Your role in scrutinising the actions of the executive is central to repairing the trust in public institutions which has been damaged on both sides of the Atlantic in recent years. My function as European Data Protection Supervisor is more modest - I seek to advise the institutions of the European Union on the impact of their actions or proposed actions on fundamental rights, particularly the rights to privacy and to data protection, Articles 7 and 8 of the Charter of Fundamental Rights.

When I mention institutions, I mean the European Parliament, the Council of Ministers of the individual Member States and the European Commission, plus another 70 separate entities. We are also increasingly invited to engage with the

[1] For a more extensive analysis on the issues, see Article 29 Working Party paper WP 228, ' Working Document on surveillance of electronic communications for intelligence and national security purposes', December 2014 and paper WP215, 'Opinion 04/2014 on surveillance of electronic communications for intelligence and national security purposes', April 2014.

European Court of Justice which is more active than ever in considering questions of privacy.

I want to talk briefly today about what, for me, is the *false dichotomy* of security versus privacy.

The concept of security has a longer heritage than that of privacy. But the historic and linguistic roots of security[2] lie not in the state watching over its citizens, but rather in the desire of the individual to be free and without care (*sine cura)*. Privacy likewise is about being left alone - and we have our American friends to thank for the early evolution of that concept, with its origins in several amendments to the US Constitution.

So in fact security and privacy are very similar ideas. Both concepts contain, at heart, the individual, and the ability to live his/her life in dignity and free from interference from others, in particular from the state.

The problem today is that security in particular is a highly contested notion. And the danger with contested notions is that every serious problem gets presented as a security problem for the state to fix, increasingly by covert means, and typically by more and more intrusive forms of surveillance.

Unfortunately, as parliamentarians like yourselves must know better than anyone else, unforeseen events can swing the pendulum towards ever greater intrusiveness.

That's why this discussion so well timed.

Only yesterday the *Assemblée nationale* of France adopted at first reading, by an overwhelming majority, a draft communications law (*projet de loi sur le renseignement*) which envisages the installation of a surveillance algorithm (*boîtes noires*/black boxes) within internet access providers, which will sift all the traffic carried over those networks for any suspicious terrorist behaviour.

[2] See, for example, Conor Gearty, *Liberty and Security,* 2014; Opinion of the European Group on Ethics in Science and New Technologies to the European Commission, 'Ethics of Security and Surveillance Technologies', 20 May 2014.

Last month, the German government proposed new guidelines on data retention requiring telecommunications and internet data to be stored for up to 10 weeks and deleted thereafter, with location to be stored for up to four weeks, and with the potential for fines against providers violating those time limits.

Last year, the UK parliament passed 'emergency' legislation, albeit with a sunset clause of December 2015, which it is claimed extended data retention requirements to over-the-top communications services such as webmail and peer-to-peer telephony.

The fact is that, in the wake of the appalling terrorist incidents in Paris in January, governments in Europe are once more under pressure to take meaningful action.

I fully recognise the need for appropriate action and legal measures. Fighting crime and terrorism are of course legitimate objectives, and data protection authorities like EDPS are not prima facie for or against any specific measure which interferes with the right to privacy and which involves handling large volumes of personal information.

The trouble, for those who fight for the rights of the individual in the EU, is that Europe has been far slower to take action on restoring trust.

On 6 June 2013, the Guardian published the first batch of Edward Snowden's disclosures of mass scale surveillance programmes.

Three months later in October 2013, shortly after it was revealed that these activities extended to monitoring the communications of politicians, EU leaders acknowledged citizens' 'deep concerns', the need for respect and trust in the work and cooperation of secret services. Two big Member States in particular undertook, by the end of 2013, to seek 'an understanding on mutual relations' with the US[3].

So nearly two years ago, evidence of massive global surveillance sparked alarm and indignation, and the EU pledged to make 'rapid' progress.

[3] European Council Conclusions, 25 October 2013.

But has anything actually changed since?

I believe that the time has come for grown-up conversation on security and privacy.

The pendulum will swing to and fro - that is the nature of politics and political discourse. But we have to start learning and applying lessons.

One such lesson was delivered by the European Court of Justice last year when it struck down the EU's Data Retention Directive, in joined cases referred by the Austrian Constitutional Court and the Irish High Court, on the grounds that the measure was disproportionate to the objectives it sought to achieve (shortly afterwards, Austria's Constitutional Court itself annulled national data protection measures on equivalent grounds). The court stated[4] that 'by adopting Directive 2006/24, the EU legislature has exceeded the limits imposed by compliance with the principle of proportionality in the light of Articles 7, 8 and 52(1) of the Charter'.

The Court, for the first time, laid down a clear series of criteria for assessing compliance of a measure in the security sphere which interferes with fundamental rights. They are of a general nature, although they were articulated in relation to the specific case of traffic data retention.

Put bluntly, the Court, applying the Charter, looks with great scepticism upon any measure which, like the Data Retention Directive, would 'appl[y] to persons for whom there is no evidence capable of suggesting that their conduct might have a link, even an indirect or remote one, with serious crime'[5].

Lawmakers in the EU now have an opportunity now to apply these criteria to all existing and future security measures.

The big test at the moment is the proposal for an EU system for processing PNR for the purposes of combating crime and terrorism, including PNR data for intra-EU flights which we know a number of national governments are insisting on.

The parallels with the Data Retention Directive are striking.

[4] Paragraph 69 of CJEU judgment of 8 April 2014 in Joined Cases C‑293/12 and C‑594/12.
[5] Paragraph 58 of judgment Joined Cases C‑293/12 and C‑594/12.

A law requiring retention of data indiscriminately on all communications became a priority in the light of the terrorist atrocities of 9/11, and top priority in 2004/5 following the bombings in Madrid and London. The directive was adopted at record speed and on the basis of little public evidence. National data retention laws based on the directive were challenged and overturned in several Member States before it eventually reached the European court.

PNR has a similar genesis and a similarly indiscriminate scope.

What about the evidence of its necessity? We know, thanks to European Parliament research, that an estimated 3 000 EU citizens are or have been foreign fighters in Syria, and that up to one in 15 (that is, 150-200 citizens) have returned to their home countries and are suspected of involvement in terrorist activities at home. I have recommended that MEPs consider whether and how PNR is relevant to this threat posed by a few hundred of their citizens.

As said to the Parliament a few months ago, the EU needs to justify why any massive, non-targeted and indiscriminate collection of data of individuals is really needed, and why, as many are arguing in the case of PNR, that measure is urgently needed now[6].

In other words, would the PNR directive have thwarted the Charlie Hebdo attacks?

Another test on the horizon is the Terrorist Finance Tracking Program, which will be in force until 1st August 2015. According to reports from the Commission (November 2013) and from the Belgian and Dutch DPAs (May 2014), there is no evidence of unlawful surveillance of the SWIFT system.

But the question this year is whether the EU can demonstrate to its citizens that the agreement is needed.

I would echo the message of the EU Counter-Terrorism Coordinator, Gilles de Kerchove, who in January wrote that "we need to focus on sustainable and long term policies".

[6] Paragraph 17 of judgment in Joined Cases C-293/12 and C-594/12.

Sustainability means being true to our values in terms of fundamental rights and freedoms. Values which I am convinced are broadly shared by all in this room.

Shared values, but a number of objective differences.

These objective differences were eloquently illustrated in an impressive speech earlier this year by Robert Litt, the General Counsel to the Office of the Director of National Intelligence[7]. In that speech Mr Litt set about to demystify the state of US surveillance and to correct misimpressions. He was at pains to emphasise the absence of 'systematic abuse or misuse' since the illegalities uncovered in the 1960s and 1970s, and explained the developments following President Obama's Policy Directive 28 of January 2014 on procedures for safeguarding personal information collected from signals intelligence activities and the recommendations of the Privacy and Civil Liberties Oversight Board in its July 2014 Report on the Surveillance Program operated under FISA.

Before I conclude, I should like briefly to highlight five of these objective differences.

First, there is the notion, expressed by governments including European ones and not only the United States, that signals intelligence activities cannot be limited to targeted collection against specific individuals who have already been identified. This is predicated on the obvious existence of unknown risks, uncovered threats, adversaries of whom we are as yet unaware, potential terrorists. As Mr Litt readily admits, bulk rather than targeted collection of this data often involves information of no ultimate value to foreign intelligence The CJEU data retention judgment, however, sets a very high threshold for justifying any such programme of indiscriminate personal data collection.

Second, there is the conviction that intelligence activities have to be kept secret to avoid compromising their ability to protect the nation. But this very secrecy also of course brings suspicion and the possibility of abuses of power.

[7] ODNI General Counsel Robert Litt's As-Prepared Remarks on Signals Intelligence Reform at the Brookings Institute, 4.2.2015.

Third, there is the argument that we should only be concerned with how personal data are 'used', and not with their collection on a massive scale. In fact Europeans' concerns and criticisms with intelligence activities are rooted not so much in fear of what the government could do with all the information it appears to be gathering – but rather the chilling effect which arises from the monitoring of the communications of millions of ordinary people.

Fourth, Mr Litt makes a striking comparison of surveillance programmes with 'an insurance policy which provides valuable protection even though you may never have to file a claim.' European case law, meanwhile, has established that traffic data generated by communications is an 'integral element on the communications made by telephone'[8]. Even 'public information' (like client telephone numbers) can fall within the scope of private life where it is systematically collected and stored by public authorities[9], and the storing of data is in itself an interference with the right to privacy, whether or not the state uses the data against the individual[10].

Fifth, there is the distinction in US surveillance rules between US citizens and everyone else. Some distinctions arise in European laws, but the distinction is far more nuanced. But ultimately under the EU Charter, there is no question that fundamental rights apply to all, irrespective of the colour of your passport. There is clearly no international consensus on privacy jurisdictional rules.

Five big differences for us to resolve: a formidable homework assignment for us all.

That's why a central component of the EDPS Strategy for the next five years, which I published in March, is to try to move this debate forward in a more mature and informed way.

Yes, we still need to conduct signals intelligence activities.

Yes, the challenges are not going away anytime soon.

[8] ECHR Malone vs UK).
[9] (ECHR, Rotaru vs Romania)
[10] ECHR Amann vs Switzerland).

Yes, state security agencies must take into account the changing technological and communications environment.

But now is the time for these agencies to implement revised targeting procedures, to specify criteria, data minimisation techniques, and to assess better the evidence available.

Now is the time to declassify documents which don't need to be kept secret, and to publish statistics summarising the effectiveness of surveillance activities.

In conclusion, you, as prominent members of your national parliaments, are entitled to demand that evidence be opened up so that we can have a proper public debate. Independent authorities like mine can then provide input which you might find helpful.

Surveillance should enhance not undermine trust in democratic institutions.

The aim of any surveillance measure must be legitimate, and its means proportionate to that aim.

In the EU Charter and data protection directive, we already have in the EU the legal tools to ensure this; we just need to apply them.

Thank you for listening.