

Data Protection, Borders and Criminal Justice: Mobile Priorities?

IN:EX LUNCHTIME BRIEFING
29 June 2010

Rapporteur: Gloria González Fuster

ABSTRACT

This report presents a summary of the discussions that took place at the INEX Lunchtime Briefing “*Data Protection, Borders and Criminal Justice: Mobile Priorities?*” on 29 June, 2010. The event was organised by the Law, Science, Technology and Society (LSTS) Research Group of the Vrije Universiteit Brussel (VUB) and the Centre for European Policy Studies (CEPS), at the CEPS offices in Brussels.



This event was organised within the framework of INEX - *Converging and conflicting ethical values in the internal/external security continuum in Europe*, a three-year project funded by the Security Programme of DG Enterprise of the European Commission's Seventh Framework Research Programme. For more information about the project, please visit: www.inexproject.eu

PROGRAMME

12.00 – 13.00: Lunch

13.00 – 15.00: Briefing panel

Opening Remarks by **Sergio Carrera** (CEPS)

Presentations

Chair: Serge Gutwirth (LSTS, VUB)

Paul De Hert (LSTS, VUB), *The US/EU Data Protection Agreement*

Cecilia Joanna Verkleij (European Commission, DG Justice, Liberty and Security), *Views from the European Commission*

Giovanni Buttarelli (European Data Protection Supervisor - EDPS), *Perspectives of the EDPS*

Jens Hjemstad (Ericsson), *Smart Borders: Smart for whom?*

Tony Bunyan (Statewatch), *Statewatch's views on Data Protection, Borders and Criminal Justice*

Open discussion

PRESENTATIONS

Sergio Carrera (Centre for European Policy Studies (CEPS)) welcomed the participants with a brief presentation of the event, as well as of the *Converging and conflicting ethical values in the internal/external security in continuum in Europe* (IN:EX) project, in the context of which the Lunchtime Briefing was organised. Introducing the topic of the day, “*Data Protection, Borders and Criminal Justice: Mobile Priorities?*”, Carrera made the point that the subject matter was undoubtedly broad, but that the discussion was, in any case, extremely timely. In this regard, the Stockholm Programme has devised a new approach to framing the issues at stake that is no longer based on a so-called ‘balance’ between liberty and security, as was customary during The Hague Programme, but on the more appropriate notion that liberty and security can only go hand in hand. This new approach, however, leaves many crucial questions open, in particular that of *whose* security is being considered when we talk about liberty and security. In other words, the questions of: what is the place of the individual in upcoming EU policies? What role is personal data protection expected to play? What about fundamental rights in general? Discussions such as those on the SWIFT agreement raise many questions, notably in relation to proportionality, oversight, and the enforceability of rights.

Serge Gutwirth (Law, Science, Technology and Society (LSTS)), Chairman of the convened panel, introduced the first speaker, **Paul De Hert (LSTS)**. De Hert gave a presentation on the legal protection of personal and transatlantic relations. Pointing out that experts on privacy and data protection from the EU and the US have been discussing these issues together in recent years, he interpreted this fact as a very positive step, and celebrated the potential of the final report of the High Level Contact Group on Information Sharing and Privacy and Personal Data Protection for further discussion. Recognising that reaching common positions on privacy and data protection across the Atlantic is far from an easy task, De Hert observed that the principles identified by the High Level Contact Group were, interestingly, extremely close to European data protection priorities. Nevertheless, some issues had been identified as pending, notably, the exact definition of a concrete institutional framework for the agreement that could at some point be negotiated, or how to relate any future general EU-US data protection agreement to existing specific agreements. In De Hert’s view, there are other crucial issues still to be resolved, such as the impact of biometrics and profiling on the US legal framework for privacy protection, which might require an update of current legal provisions.

Four areas were described by De Hert as needing special attention in the future: the question of data protection authorities, which must be independent, as EU institutions regularly state, but also need to be effective; the notion of data minimisation, in particular in light of massive demands of data; the legal concept of proportionality and its implications, and, lastly, profiling and the regulation thereof.

The next speaker, **Jens Hjelmsstad (Ericsson)**, opened his intervention with a few words about the company he works for, Ericsson, and its background in the areas of telecommunications, data protection and data exploitation. Hjelmsstad focused on the possible links between telecommunications and border control, and on how such a relationship could lead to the tracking of individuals, with potentially very dangerous consequences. In this context, he observed, private companies need to reflect carefully

on the need for the private sector to follow certain rules, which explains why Ericsson is a partner in the INEX project.

Referring to the INEX Paper "*Intelligent Human Filtering at Europe's External Borders*", co-authored by himself, Erling Jensen and Espen Vagran, he described different practices of border monitoring in Europe and how controls at the points of entry have evolved, in particular due to Schengen requirements. He commented that the reliance on biometrics combined with remote identification could reduce the chances of crossing 'green borders' (the rural areas with reduced traffic between allocated entry/exit points), but, at the same time, they problematically blur the difference between 'green borders' and points of entry. In 'grey borders' (the more densely populated areas adjacent to entry/exit points), border control could also cause other problems – seriously affecting local life and business, for example.

Hjelmstad also reflected upon the relationship between physical walls and electronic monitoring, and expressed the view that in the area of border control companies might face many specific demands from the 'customers' of these services. Lastly, he emphasised that some companies access data that could, technically, be used to develop powerful profiling systems, so it is critical to discuss openly how this should be controlled; the ultimate question, in his view, being: for whom are smart 'smart borders' intended?

Tony Bunyan (Statewatch) began his presentation by examining the view that, since the events of 9/11, a 'balancing' of security and liberty has been taking place. Taking into account actual developments, he noted, it must be acknowledged that such an alleged 'balancing' act has actually meant that security has been systematically privileged, to a point that it has become embedded in the EU ethos. The new mantra of the Stockholm Programme, revolving around fundamental rights, should not distract attention from the necessity of reviewing the measures taken since 9/11.

As EU institutions insist on mentioning European 'common values', there is a need to question what those values are, Bunyan argued; even in academic circles, discussions about Europeanisation sometimes neglect the fight for real democracy. As multi-governance theories proliferate, they seem not to consider all the practices necessary to ensure that the development of state measures meets the requirements of genuinely democratic states. For instance, even though the European Parliament has recently acquired new powers, it is still solely concerned with discussing upcoming laws.

Regarding existing and currently discussed measures, Bunyan cautioned that one should always consider who is being targeted by the measures adopted: in particular, people such as Muslims or asylum-seekers, but also other individuals, for instance those generally categorised as 'radical'.

On the subject of data protection, Bunyan's view was that the existing legislation does not fulfil its objectives. He noted that EU data protection law should be about data control, but, in practice, no one has control over their own data. Bunyan described three types of identity – first, an identity that is known to us; second, a digital identity constructed by the state, and, third, a digital identity constructed by multinationals, adding that access to the last two is not granted to individuals. Not only those dealing with 'security' use this fact as a trapdoor to avoid protection, but, worryingly, multinationals appear to perceive the personal data that they process as 'their data'.

All these developments might initially affect third country nationals, but will eventually have an impact on all citizens, Bunyan warned, citing data retention as an example of

mainstreaming of this type of measures. He declared that the EU has become one of the areas in the world with the most surveillance, with highly intrusive practices being implemented due to US pressure. As a result we are now living in an authoritarian state, in a surveillance society, but that as these are both still 'under construction', this evolution is not being perceived as such by the general population. Nevertheless, Bunyan stated, because these measures are being implemented now, something needs to be done now, before it is too late.

Giovanni Buttarelli (Assistant Supervisor of the European Data Protection Supervisor (EDPS)) celebrated the timely nature of the event, as the European Commission was at that very moment discussing the future of EU data protection. Buttarelli observed that the topic of the day was very broad, and that many different aspects could be discussed, either in relation to European data protection in the past, the present, or the future. Regarding the present, he observed, one could discuss the added value of the Reform Treaty, for instance, which leads the way to a new phase in the evolution of data protection in Europe, an enforceable right to personal data protection is now recognised as such. This right is accompanied by a series of principles, such as the purpose limitation principle, or the proportionality and necessity principles, which are to be duly taken into account when discussing policy measures, as the EDPS regularly notes, he added, underscoring that the principles now need to be applied intelligently.

Buttarelli then considered the future of European data protection, and the fact that EU institutions are now dealing with a demanding legal base, which imposes the need for a comprehensive legal framework, and which could take into consideration the need to reduce the margin of action left to Member States in some regards. But challenges do not only arise from recent legislative developments, Buttarelli stressed, referring to the fact that the courts are also contributing to change, as well as to the notion of a new 'information management strategy' being discussed by EU institutions. The EDPS has repeatedly called for the identification of a global strategy for data processing, as well as for the technical and technological implementation of the principle '*select before you collect*'.

There are areas in which developments are far from being promising, Buttarelli warned, mentioning the case of FRONTEX, in which the possibility to process personal data is being introduced in a very opaque manner, without clear recognition of the crucial need for personal data protection. Buttarelli concluded by pointing out that, although we might already be living in a surveillance society, we also have the right to place under surveillance those who opt for surveillance.

Part of the **discussion time** was devoted to a debate on the possible ways to encourage an informed debate on these issues, and on how even small communication improvements by EU institutions could have huge repercussions. Other subjects discussed were the market for Privacy Enhancing Technologies (PETs), the possible forms of the US/EU data protection agreement and its possible binding effect, the relation between data protection and access to documents, the regulation of profiling, data protection obligations of search engine providers, and the notion of interoperability.