

Data Transfers in the New AFSJ: Go with the Flow? Converging and Conflicting Ethical Values in the External/Internal Security Continuum in Europe

Proceedings of an IN:EX Workshop 10 May 2010

Rapporteurs: Erika Ellyne, Rocco Bellanova and Gloria González Fuster

ABSTRACT

This report offers a synthesis of the proceedings and discussions that took place during the workshop “*Data Transfers in the New AFSJ: Go with the Flow? Converging and Conflicting Ethical Values in the External/Internal Security Continuum in Europe*” on 10 May 2010 at CEPS in Brussels.

Organised by the Law, Science, Technology and Society (LSTS) Research Group of the Vrije Universiteit Brussel (VUB), in cooperation with the Justice and Home Affairs Section at CEPS, the workshop brought together policy-makers, civil society representatives and researchers.



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

10.30 – 11.00: REGISTRATION

11.00 – 11.15: WELCOME ADDRESS

- Sergio Carrera (CEPS) and Serge Gutwirth (LSTS)

11.15 – 13.00: EXISTING AND UPCOMING INFORMATION PROCESSING PRACTICES IN THE NEW AREA OF FREEDOM OF SECURITY AND JUSTICE

- **Chair:** Serge Gutwirth (LSTS)
- Jan Philipp Albrecht (MEP)
- Alfonso Scirocco (EDPS)
- Patrick Beyer (AK Vorrat)

Discussion time

13.00 – 14.00: Lunch

14.00 – 15.45: DIGITAL RIGHTS AND DIGITAL BORDERS

- **Chair:** Julien Jeandesboz (Sciences Po)
- James Thurman (DETECTER Project)
- Katarzyna Cuadrat Grzybowska (EDPS)
- Juliet Lodge (Leeds University)
- Joe McNamee (EDRI)

Discussion time

15.45 – 16.00: Coffee Break

16.00 – 17.45: GLOBAL DATA TRANSFERS

- **Chair:** Peter Burgess (PRIO)
- Elspeth Guild (CEPS)
- Claire Gayrel (FUNDP)
- Paul De Hert (VUB, Tilburg University)

Discussion time

17.45 – 18.00: CONCLUDING REMARKS

- Peter Burgess (PRIO)

Data Transfers in the New AFSJ: Go with the Flow?

Converging and Conflicting Ethical Values in the External/Internal Security Continuum in Europe

Proceedings of an IN:EX Workshop
10 May 2010

Rapporteurs: Erika Ellyne, Rocco Bellanova and Gloria González Fuster

The welcome and opening remarks to the workshop were given by **Sergio Carrera**, who explained that, in the context of the IN:EX Project (*Converging and conflicting ethical values in the internal/external security continuum in Europe*), the Law, Science, Technology and Society (LSTS) Research Group of the Vrije Universiteit Brussels and the Centre for European Policy Studies (CEPS) are cooperating in the organisation of a series of Lunchtime Briefings.

Carrera briefly reviewed the main features of the situation that the European Union (EU) is now experiencing, which he characterised as “fascinating” and which could have great repercussions on European data protection. First, he stressed that there is currently a new political framework, due to the adoption of the Stockholm programme, and the implementation of this programme could reveal unprecedented tensions between the Council and the European Commission. Second, a new legal framework is now in place, as established by the Lisbon Treaty. In this legal framework, the protection of personal data acquires particular relevance, as already stressed by the European Data Protection Supervisor (EDPS). This new situation should materialise in four concrete actions foreseen by the European Commission in its action plan to implement the Stockholm programme. All in all, developments show that there is no longer a pressure to balance security against fundamental rights, but that fundamental rights represent the premise for the future of the Area of Freedom, Security and Justice (AFSJ).

Panel I: Existing and upcoming information processing practices in the new Area of Freedom of Security and Justice (AFSJ)

Serge Gutwirth, chair of the first panel, introduced the speakers and excused the absence of Despina Vassiliadou.

Alfonso Scirocco, legal advisor at the EDPS, opened the panel session with a presentation on *“Data Protection Before and After Lisbon”*. The first part of his intervention gave an overview of the state of data protection in the EU before the entry into force of the Lisbon Treaty. He recalled that, under the pillar system, the main component of EU data protection was the Directive 95/46/EC, a provision that was accompanied by various sectoral measures (such as the Directive 97/66/EC, later replaced by Directive 2002/58/EC and recently amended). The European Court of Justice (ECJ), through its case law, had clarified that the scope of Directive 95/46/EC was broad, and not limited to processing undertaken in the context of purely economic activities (contrary to opinions such as those expressed at the

time by Advocate General Tizzano), thus contributing to the progressive transformation of data protection into a fundamental right. The second and third pillars were distinct legal arenas. The third pillar was a motley patchwork of regulations. Though Article 30.1.b of the EU Treaty called for the collection, storage and processing of relevant information in the field of police cooperation to be "*subject to appropriate provisions on the protection of personal data*", for a long time no general framework could be adopted as unanimity was difficult to achieve. This led to a lowest common denominator approach, and it was only possible to elaborate rules for specific sectors in specific initiatives, i.e. Europol, Schengen, Eurojust, Prüm. Eventually a framework decision was adopted, but with no satisfactory results from the EDPS perspective. Regarding the second pillar, even more intergovernmental in nature, there was no article whatsoever referring to data protection. However, the ECJ case law on so-called 'terrorist black lists' (which should more accurately be referred to as 'lists of suspected terrorists') can be considered relevant on the matter, as, even though there was no explicit mention of data protection rights, it can be interpreted that in these cases the Court does refer to the right to access personal data, and thus, in a way, to data protection.

Scirocco continued his presentation by describing some currently important trends in relation to data processing. He underlined that data, including commercial data, are increasingly collected for law enforcement purposes, and that in this respect we are witnessing a shift from public to private law enforcement. On another level, the European Court of Human Rights (ECtHR) has been particularly active in addressing the substance of the data protection, for instance in the *Marper* judgment. Due to globalisation, relations with third countries become a crucial issue, and in particular one must consider whether third countries can be given the power to dictate EU internal law enforcement strategies (for instance, in relation to financial monitoring). With the advent of the Lisbon Treaty, Article 16 of the Treaty on the Functioning of the European Union (TFEU) establishes a new horizontal legal basis for data protection across all pillars, and the Charter of Fundamental Rights of the European Union, which institutes data protection as a fundamental right in its Article 8, becomes binding. The EDPS reads this as having direct effect, thus granting data protection rights across all pillars. Recently, the ECJ has clarified the importance of the independence of data protection authorities. In the future, data protection needs to be built into any upcoming data exchange system, embedded in upcoming architectures; 'interoperability' choices should be questioned, as not everything that is technologically possible is legally possible. Furthermore, a solution is needed for data protection concerns when commercial data is used for security purposes. In Scirocco's view, the European Commission should be ambitious in future substantive issues and in its institutional framework.

Patrick Breyer gave a presentation titled "*How Ethical is Looking Away? Ethical Dilemmas of the Secrecy of Telecommunications*", during which he examined the ethical dimensions related to the monitoring of communications. Taking as a starting point the fact that German data retention provisions were recently judged unconstitutional by the German Constitutional Court, he analysed the possible benefits of data retention. Breyer discussed the different types of cyber crime and how data retention practices do not translate into any remarkable increases of the number of cyber crimes resolved. Moreover, he explained that there are similar types of off-line crime and behaviour, which cannot be traced, and that, in any case, there are other ways of tracking this type of crime than data retention; in

general, certain behaviour is not traceable because as a society we do not wish it to be so in everyday life. He then considered the question of how ethical it can be to look away from the consequences engendered by data retention. In this context, he pointed out that data retention reduces access to help, as, for instance, anonymous crisis hotlines lose callers, due to the fear that real anonymity of the calls might be no longer ensured, and that it can also deter press sources and whistle-blowers. Moreover, one needs to remember, he insisted, that reputations are quickly shattered and data retention is prone to error. Finally, Breyer argued that data retention changes the very foundations of society, modifying the way society works, and that there is no solid justification to let that change happen. Looking away, he concluded, can be generally considered a more ethical approach than not looking away.

Jan Albrecht opened his intervention with a few words on Foucault's description of the *panopticon*. Albrecht declared that he is particularly concerned with the implications of surveillance for the rule of law and, more broadly, for democracy, as surveillance practices have an impact on the relationship between the individual and the state. Describing the situation that the EU is currently going through, he underlined that there is much uncertainty and instability: too many legal provisions of the third pillar, as well as international agreements, suffer from a lack of parliamentary debate, be it at European or national level. In his opinion, the new powers granted to the European Parliament will help to re-open long due debates. The rights to privacy and personal data protection are fundamental rights by themselves but they are, moreover, closely related to other fundamental rights, such as freedom of expression. Ensuring such rights is essential, and thus, the EU needs to guarantee at least a common minimum protection, regardless of possibly divergent national approaches. Furthermore, there are a number of important fields in which the EU still has a lot to do, such as criminal law and, more particularly, procedural criminal law. Regarding legal protection, he commented that over the last decades the notion of 'proportionality' has not been treated with enough precision, as words such as 'effectiveness' and 'necessity' have too often been used without solid ground or any convincing explanation – the time has come to clarify their meaning in sufficient detail. Lastly, Albrecht urged for a closer examination of all these issues, to accompany the future efforts of the legislator, and insisted on the idea that behind all these discussions there is the political problem of identifying what needs to be done to fight criminality.

Discussion time was devoted to various subjects. The audience and the speakers reflected upon the possible need for simpler rules, or principles, and upon the extent to which these fundamental principles are already in place in Europe or not. Peter Burgess observed that crime-fighting has fundamentally been altered in recent years, marking a shift from a pre-crime to a post-crime, 'fictional', pre-emptive approach, and located the roots of this process in the development of US marketing strategies, which led to a lively discussion on the current value of fact-based decision-making. The future of data protection was also briefly debated, and in this context the usefulness of a concept such as 'privacy-by-design' was questioned. Elspeth Guild manifested her astonishment at the current disconnect between the transparency imposed on individuals and the extremely limited transparency of the state.

Panel II: Digital rights and digital borders

Julien Jeandesboz, chair of the second panel, introduced the speakers.

James Thurman presented his work, carried out in the context of the DETECTER project, on the use of detection technologies in the fight against terrorism, and, more concretely, on the use of data mining and profiling in border situations. Firstly, he addressed the question of the definition of data mining, indicating that there are many different definitions, some narrow, some broad; the former limit data mining to predictive practices or to the reliance on probabilistic algorithms, whereas the latter covers any kind of automated analysis aimed at revealing relationships or summarising large sets of data. The practices referred to often rely on the use of statistical analysis, clustering (finding groupings of data items within one or more sets of data), link analysis (revealing relationships between data items) or pattern analysis (identifying patterns within data).

Thurman mentioned the CAPPs project as an American example of data mining in a cross-border context. CAPPs applied a certain set of 'rules' to identify individuals of potential interest, 'rules' being a "*set of weighted characteristics and behaviors (...) that TSA has determined correlate closely with the characteristics and behaviors of terrorists*". It was foreseen that the CAPPsII project, now replaced by the Secure Flight programme, would rely on an expanded set of factors, and reports suggest that it would have involved access to data from both government and commercial databases. In addition, cross-referencing with watch lists was planned there, though the real data mining element would have sought to uncover new terrorist suspects based on patterns in travel and transactional data. Another example mentioned was the Automated Targeting System, used by customs and border control, which has also come to include cross referencing with Passenger Name Records (PNR) Data and vehicle registration information for ground entry. Other examples included two systems used by Immigration and Customs Enforcement: NETLEADS, providing search capabilities over multiple databases and trend and pattern analysis (which accesses data from the internal Homeland Security databases and some public sources, including news feeds) and ICEPIC, a system with access to numerous government databases, in particular databases maintained by Homeland Security, providing simple search capabilities and relationship analysis, and revealing connections between people.

The risks and issues that lie behind data mining are manifold, explained Thurman, mentioning the abuse of police powers, false positives and false negatives; security issues such as the risks of breach from inside or outside, or the risks involved in data transfer and sharing. In a human rights perspective, he alluded to the serious threats to equality and the presumption of innocence through, respectively, unlawful discrimination and guilt by association. Moreover, he referred to the worrying trend of increasing use of commercial databases for security purposes. In his view, excessive focus on the term 'data mining' can distract from considering a series of important issues, and it could be more beneficial to aim at establishing a general framework for all data handling, which should address not only the collection of information, but access to the databases, sharing of data, security, retention, system architecture and oversight.

In her presentation, **Katarzyna Cuadrat Grzybowska** discussed data protection as a pre-condition for efficient border management and for the successful use of new technologies, as well as data protection principles relevant to digital borders and

the use of biometrics, and the notions of proportionality and necessity. Data protection, explained Cuadrat Grzybowska, is not only a fundamental right, but also a pre-condition to mutual trust between authorities and a guarantee of effective border management, not an obstacle to border security. In this context, she briefly described the EDPS' mission, which is notably to ensure the protection of people whose data are processed by the Community institutions and bodies and give advice on new legislation that has data protection implications, the three main functions of the EDPS being that of supervision, consultation, and cooperation. The EDPS, she recalled, has issued various opinions on legislative proposals related to border management, and, in terms of cooperation, the EDPS cooperates actively with national data protection authorities, notably by undertaking *coordinated supervision* for Eurodac. On Eurodac, she pointed out that different questions pertaining to who has access to Eurodac arise, especially with regard to law enforcement authorities. Additionally, the Eurodac Supervision Coordination Group has produced a Second Inspection Report on information for data subjects and the age assessment of young asylum seekers.

Cuadrat Grzybowska recounted that data protection is encapsulated under Article 8 of the European Convention of Human Rights (ECHR), as data processing may interfere with the right to respect for private life. As such, it is also subject to the traditional principles that govern possible interferences with the right; the *Marper* judgement provides especially useful information on how the proportionality test can be applied to the use of biometric data. Moreover, data protection as an autonomous right has been instituted by the Charter of Fundamental Rights in its Article 8. With regard to data protection, she noted that border control involves privacy-intrusive measures and the collection of a vast amount of data; such interferences must be laid down by law, foreseeable, necessary to achieve the public interest pursued, and have a clear purpose. There must be evidence that a measure is necessary, meaning as unobtrusive as possible. Finally, she recalled that the EDPS has also rendered an opinion on the Stockholm programme and that the EU seems to be heading towards the creation of a European information model. In this context, choosing the right architecture and safeguards is of prime importance, and a series of questions as to what to do with information collected for other purposes or the use of biometrics is also to be answered. In conclusion, she emphasised the need for an open democratic debate, with clear and careful policy choices, to rely on the prior assessment of existing instruments.

Juliet Lodge began a presentation titled "*Quantum Surveillance and 'Shared Secrets', a Biometric Step too Far?*" by asserting that new information technology is to transform society, and that, although technology tends to be accepted as a good thing, some technological advancement opens the door to risky behaviour and creates a false impression of security. In this sense, she observed that there are too many negative consequences of biometrics; discrimination, privacy issues, arbitrary, unethical and disproportionate *insecuritisation* of citizens, and that the US support to the use of biometrics has led to new ways of tracking people. Despite judging that the use of biometrics can be highly risky, leading to 'quantum surveillance', she questioned the opportunity of reacting to this trend by relying on so-called Privacy Enhancing Technologies (PETs), which can be described as a privatisation of privacy and carry their own risks in terms of discrimination. In the end, Lodge claimed, and as we witness a progressive process of de-contextualisation, de-politicisation and de-humanisation of new spaces of

governance, the question might be to identify who is in control. The trust deficit between state and individuals has been widening because of prioritising form over substance; in this regard, the safeguards in place against the abuse of trust and power are inadequate. In her view, the use of biometrics changes the meaning of identity, and automated decision-making, which we have come to rely heavily upon in the biometrics sphere, is also changing the dynamic between man and machine. All this challenges our capacity to control society in a democratic and ethically acceptable fashion.

Biometrics is the information and communication technologies' (ICT) answer to border control to sort and confirm identity, Lodge asserted, adding that ideally its applications would allow the identification of persons in rescue missions (such as disaster relief), but that in a dystopian scenario there is also the possibility for biometrics to be used as a pharmaceutical enhancement of cognition, memory, mood and related functions or to manipulate memory, including erasure or moderation of traumatic memories. The current disproportionate use of biometrics makes context proportionality always contingent, and it can be questioned whose contingency is reflected by perceptions of risk to privacy and security – man or machine's? ICTs are used to identify in and out groupers, Lodge asserted, and, in the process, we have come to rely heavily upon automated decision-making based on mathematical algorithms that we take as infallible and we believe in the existence of one unique identity and loyalty, which does not reflect reality. This has led to disaffection, democratic deficit, alienation, and distrust. As a result there is a new set of out-groupers, the alienated. Among the questions to be addressed in this context, are: what is the solution? Can communication do without human intervention? Under what circumstances? To what end? With what result? Many ancillary and shadow data can be generated by behavioural multimodal biometric ICTs, which have a high potential for misuse.

In Lodge's opinion, identity has become the preserve of global machine-led processes; society has privatised unaccountability and put machines in charge. Thus, shifts in governance at the physical and legal borders of Europe risk a 'loss of accountability'. Although there is still very little legislation or case-law on proportionality in relation to use of biometrics, the ICT impact is not neutral, and there are numerous ethical problems behind automated decision-making. Misperceptions and presumptions of certainty compromise discretionary access and disclosure. As neuroscience is being used as part of biometrics, how and what we think is slowly seeping into new forms of biometrics. Personal identity is crucial for the attribution of moral responsibility, Lodge opined and, therefore, there might be a contradiction between the data subject as data controller (in social networking), enjoying individual responsibility, and the data subject as commodity with no individual right or responsibility for giving consent to the use of his personal data. Finally, Lodge declared that biometrics introduces problems of trust, accountability and credibility, and obliges one to question the kind of society we are heading towards.

Joe McNamee first described the *big bang* that took place with the digital revolution, making some borders disappear for the best, while other, new borders appeared. Prior to the *big bang*, data was stored when it was actually necessary, whereas today it can be stored for no particular reason. In this respect, the principle of necessity, useful in theory, is in practice not well implemented. According to McNamee, the European Commission has failed to conduct any satisfactory impact

assessment of measures in relation to human rights, and this has happened despite the highly problematic nature of some of the proposed measures. He underlined that the existence of a legal framework for the protection of personal data does not guarantee that provisions are enforced, and suggested that nowadays companies can easily choose not to respect existing provisions. Concretely, he denounced how 'proportionality' loses its meaning as service providers unilaterally decide to store data for long periods of time, as well as how general conditions of acceptance can be extremely long and packed with legal jargon, begging the question of whether one can really speak of 'informed consent' of the data subject. McNamee commented, among other issues, on the subject of internet monitoring and blocking, for instance in relation to the fight against child exploitation, described general developments related to the progressive privatisation of policing, and highlighted the risks of function-creep related to these practices. Additionally, he observed that public authorities are at the same time supporting these policies and the development of technologies that allow a circumvention of them, notably through research funding.

During the **discussion time** many related subjects were given detailed consideration, such as: the relation between data mining and biometrics, the need to question the very necessity of designing an 'EU information model'; the opportunities and challenges of the ongoing discussions on the EU's fundamental rights architecture, the convenience of defining the notion of data mining. The discussions were particularly lively in relation to the issue of who should be the prime concern of privacy and data protection laws, and how to relate the categories *citizens vs. individuals* and *third country nationals vs. vulnerable third country nationals* to these subjects.

Panel III: Global data transfers

Peter Burgess, in his role as chair of the panel, welcomed the speakers.

Paul De Hert addressed the issue of personal data protection from a transatlantic perspective, taking as a starting point his research work carried out together with Rocco Bellanova. As explained by De Hert, in the EU there are currently two separate rights: a right to privacy and a right to the protection of personal data. Article 8 of the EU Charter of Fundamental Rights establishes that the processing of personal data should be 'fair': this requirement has an ethical background and is thus recognised at a very high level in the EU legal framework. The current question in the area of transatlantic cooperation is how to envisage security-related cooperation as traditional cooperation through criminal law is not a possibility.

De Hert contrasted this with the situation of data protection in the US, where there is no constitutional right to the protection of personal data. Comparing key case-law from both sides of the Atlantic, he stressed the weak status of privacy in the US, notably due to the use of the notion of 'expectations of privacy'. Although there are important laws on privacy in the US that establish important principles, they contain a series of troublesome details. Three main problems can be identified: a) the use of the notion of 'system of records'; b) the fact that rights are only awarded to US citizens; and c) the reliance on broad notions to allow processing practices. Moreover, traditionally the fact that there is no independent supervision has also been considered a major problem, but this idea might need to be nuanced (as done

by Rotenberg). Ultimately, the situation in the US cannot be considered fully satisfactory.

Elsbeth Guild began her intervention by describing what is ultimately at stake when we discuss global data transfers. In that sense, she recalled that for a number of persons the reliance on inaccurate data transferred across borders has had dramatic consequences, sometimes resulting in lives being destroyed (as was the case for Maher Arar, for instance). Therefore, she emphasised that data transfers are not innocent. The starting point of our thinking on these issues, she argued, should be the question of what data can be collected and how, which leads to the question of the eventual pressure to share the data collected and the issue of what is legitimate to hold in a database. These reflexions led her to a discussion of the *Marper* case, in which the European Court of Human Rights examined the storage of three different kinds of data: DNA profiles, cellular samples and fingerprint data. In that judgement, the Court was obliged to analyse how such storage related to privacy. Guild reviewed the reasoning followed by the Court and noted that several problems were identified in the relevant UK measures. Moreover, she underlined that the major ill described by the Court was the stigmatisation of those whose data was stored.

Claire Gayrel's presentation dealt with the purpose limitation principle and its erosion in the Area of Freedom, Security and Justice (AFSJ). She started her intervention by highlighting that the purpose limitation principle is a central element of Convention 108. The main objectives of the principle are to counter practices such as those encouraged by the notion of interoperability. However, the trend in the AFSJ is to consider many different secondary purposes compatible with the original purpose of collection of data. This widening of uses can include the use for law enforcement purposes of commercial data, as well as relate to international data transfers. Regarding transfers to the US, the ultimate question is how detailed a description of allowed purposes can be that does not define 'compatible purposes'. This discussion, moreover, needs to be linked to the issue of informed consent, as it does have an impact on the possible consent of data subjects to have their data processed.

The **discussion time** allowed for further debate on the issue of possible ways to think about the consequences of applying the purpose limitation in the AFSJ. Moreover, the subject of the possible re-use of data available on the internet for purposes not originally foreseen was also considered.

Peter Burgess concluded the event with a few reflexions on the INEX project. INEX, he recalled, is a multidisciplinary project that has as one of its general objectives to consider the larger picture of contemporary transformations of the person, concretely through the relation of the person with technology, when discussing security. In this sense, the analysis of the current evolution of the EU internal security strategy reveals that different important ethical considerations are missing from current debates. Burgess stressed that the INEX project is now reaching a key moment, in which it must aim at maximising its impact, and that the INEX Lunchtime Briefings can play a very important role in reaching this objective.