"Surveillance, Privacy and Security: A large scale participatory assessment of criteria and factors determining acceptability and acceptance of security technologies in Europe"

Project acronym: **SurPRISE**

Collaborative Project

Grant Agreement No.: 285492

FP7 Call Topic: SEC-2011.6.5-2: The Relationship Between Human Privacy And Security

Start of project: February 2012

Duration: 36 Months

D 3.2 – Report on regulatory frameworks concerning privacy and the evolution of the norm of the right to privacy

Lead Beneficiary: EUI

Author(s): Maria Grazia Porcedda (EUI), Martin Scheinin (EUI), Mathias Vermeulen (EUI)

Due Date: January 2013

Submission Date: March 2013

Dissemination Level: Public

Version: 1

This document was developed by the SurPRISE project (http://www.surprise-project.eu), co-funded within the Seventh Framework Program (FP7). SurPRISE re-examines the relationship between security and privacy. SurPRISE will provide new insights into the relation between surveillance, privacy and security, taking into account the European citizens' perspective as a central element. It will also explore options for less privacy infringing security technologies and for non-surveillance oriented security solutions, aiming at better informed debates of security policies.

The SurPRISE project is conducted by a consortium consisting of the following partners:

Institut für Technikfolgen-Abschätzung / Oesterreichische Akademie der Wissenschaften Coordinator, Austria	ITA/OEAW	
Agencia de Protección de Datos de la Comunidad de Madrid*, Spain	APDCM	
Instituto de Politicas y Bienes Publicos/ Agencia Estatal Consejo Superior de Investigaciones Científicas, Spain	CSIC	
Teknologirådet - The Danish Board of Technology Foundation, Denmark	DBT	
European University Institute, Italy	EUI	
Verein für Rechts-und Kriminalsoziologie, Austria	IRKS	
Median Opinion and Market Research Limited Company, Hungary	Median	
Teknologirådet - The Norwegian Board of Technology, Norway	NBT	
The Open University, United Kingdom	OU	
TA-SWISS / Akademien der Wissenschaften Schweiz, Switzerland	TA-SWISS	
Unabhängiges Landeszentrum für Datenschutz, Germany	ULD	

*APDCM, the Agencia de Protección de Datos de la Comunidad de Madrid (Data Protection Agency of the Community of Madrid) participated as consortium partner in the SurPRISE project till 31st of December 2012. As a consequence of austerity policies in Spain APDCM was terminated at the end of 2012.

Table of Contents

List of Abbreviations

Abbreviation	Meaning
AFSJ	Area of Freedom, Security and Justice
CoE	Council of Europe
CFSP	Common Foreign and Security Policy
DPI	Deep-packet inspection
ECHR	European Convention of Human Rights
ECJ	Court of Justice of the European Union
EU	European Union
EUCFR	European Charter of Fundamental Rights
FIP	Fair Information Principle
HRC	Human Rights Committee
ICCPR	International Covenant of Civil and Political Rights
LEAs	Law Enforcement Agencies
OECD	Organization for Economic Cooperation and Development
PbD	Privacy by Design
PPP	Public-private partnership
SOSS	Surveillance-oriented security solution
SOST	Surveillance-oriented security technology
TEU	Treaty on the European Union
TFEU	Treaty on the Functioning of the European Union
UDHR	Universal Declaration of Human Rights

Executive Summary

Aims of the deliverable

This deliverable reviews the current state of, and explores challenges and options for, political and legal developments concerning privacy and security in the European Union (EU). In particular, it scrutinizes the legal dimensions of the so-called 'security vs. privacy' trade-off, whereby security and rights are deemed irreconcilable interests, and security often trumps rights due to its purported overarching societal weight.

The deliverable provides a detailed comparative review and analysis of recent judgments and legislation in the field of privacy and surveillance-oriented security solutions and technologies (SOSSs and SOSTs), in order to achieve three immediate objectives. Firstly, capturing the norm of the fundamental right to privacy (and, where appropriate, the norm of the fundamental right to the protection of personal data); secondly, determining the legal permissibility of restrictions applied to this right; and finally, reflecting upon European judgments in which the right to privacy was 'balanced' with the need to provide security.

Appraising the legal dimensions of the security vs. privacy approach (section 1.3)

The deliverable challenges the assumption that the collective interest to security and the rights to privacy (and data protection) are irreconcilable in the EU, as results in particular from the exponential increase of intelligence-led policing after 9/11, which led to the routine use of SOSTs and SOSSs. In the security context, surveillance comprises the targeted or systematic monitoring, by governmental organizations and their partners, of persons, places, items, infrastructures or flows of information, in order to identify hazards and manage risks and to enable, typically, a preventive, protective or reactive response, or the collection of data for preparing such a response in the future. The policies regulating the adoption of SOSTs framed the relationship between privacy (together with data protection) and security predominantly in terms of the need to 'strike a balance' or establish a 'trade-off' between security and rights, as two societal values that sometimes may end up in tension with each other. The ensuing restrictions imposed on the two fundamental rights for the purpose of security have arguably exceeded the permissible scope of limitations to both rights so that it can be questioned whether all resulting limitations are actually compatible with the values these rights seek to protect.

This should not be the outcome, as the EU is "founded on the values of respect for human dignity, freedom, democracy, equality, the rule of law and respect for human rights, " which include the rights to privacy and data protection. As acknowledged by the Court of Justice of the European Union, "The fundamental rights recognized by the Court are not absolute (…). Consequently, restrictions may be imposed on the exercise of those rights (…) provided that those restrictions in fact correspond to objectives of general interest pursued by the Community and do not constitute, with regard to the aim pursued, a disproportionate and intolerable interference, impairing the very substance of those rights." Objectives of general interest, or aims, pursued by the EU are the promotion of peace, the preservation of its traditions and citizens' well-being. The first consequence is the creation of an internal, borderless area, protecting citizens' fundamental rights, guaranteeing a high level of security and fostering access to justice, in respect of the different legal systems and traditions proper of member states: the Area of Freedom, Security and Justice (hereafter AFSJ).

Consequently, security is instrumental to the pursuit of the objective of general interests by the EU, and the protection of fundamental rights, including the right to privacy and data protection, and can be seen as a public good. The protection of public or national security is thus seen as a legitimate aim justifying restrictions on the exercise of the rights under analysis in a democratic society.

Security as a contested concept (section 1.3)

Part of the problem of the security vs. privacy debate lies in the contested nature of the concepts under analysis. 'Security' is vaguely referred to in the TEU in articles 3.2 and 3.5, 21.2 (a) and (c) AFSJ-related policy documents describe it through threats "which have a direct impact on the

lives, safety, and well-being of citizens." Threats are usually grouped in broad categories, which inform the basis of policy making in the AFSJ, and include "serious and organised crime, terrorism, drugs, trafficking in human beings and smuggling of persons" as well as "cybercrime, the management of…external borders and…natural and man-made disasters." The vagueness of the concept, coupled with the emotional thrust for strong responses in the wake of security failures, such as terrorist attacks, have led to the adoption of policies based on the extensive processing of personal information, which claim to 'strike a balance', i.e. weigh fairly security interests and privacy (and data protection) rights, but de facto result in introducing excessive limitations to such rights, questioning their significance in our society.

Privacy and data protection as contested fundamental rights: legal evolution and permissible limitations (section 2.1)

The deliverable highlights two defining elements of the right to privacy that may be seen as informing its social significance and consequent legal development. On the one hand, privacy is understood as a right to personality or identity, a right entrusting "individuals and groups to be able to think and develop ideas and relationships", thus serving as a meta-right, as the basis for civil and political rights such as freedom of expression, association, and movement, which could not be effectively enjoyed otherwise. On the other hand, privacy puts normative limits to such technological advances and related practices that interfere with autonomy and freedom (home, body and correspondence). The internationalization of privacy threats allowed by trans-border data flows further informed its legal development.

Fundamental rights, already enshrined in many constitutions, informed the legislative development of the right to privacy, formally initiated by the adoption of the Universal Declaration of Human Rights (UDHR) 1948. The latest formulation of the rights to privacy and data protection is enshrined in articles 7 and 8 of the European Charter of Fundamental Rights (hereafter EUCFR). These two articles incorporate the progresses made by earlier instruments applicable in the EU. Consequently, it can be argued that the three main functions performed by all relevant instruments (formulation, protection mechanisms and limits) should be read together.

Definitions. The first formulations of the right to privacy attest to its universal relevance. 'Privacy' appears as an umbrella term encompassing the protection of mental and physical (spatial and bodily) integrity, intimate relationships, and information relating to such spheres, often grouped into four categories of privacy: bodily, relational, informational and territorial. Courts (and legal scholarship/jurisprudence) upheld and contributed to this versatile understanding. Informational privacy, or the right to personal data protection, has been the object of the most recent legal instruments, and is defined in more procedural terms. The OECD Privacy Guidelines introduced the Fair Information Principles (FIPs), which regulate the processing of the data and were 'officialised' by the Council of Europe Convention 108. Convention 108 further introduced the category of sensitive data, i.e. data that should not be processed unless specific safeguards apply. Directive 95/46/EC and 2002/58/EC built on these two texts to refine the definition of personal data and the architecture surrounding them.

Mechanisms of protection. Article 12 UDHR, 8 ECHR and 17 ICCPR refer to the activity of the state. They clarify that states are under the legal obligation to refrain from unduly interfering with the right to privacy, and have positive obligations to take the necessary legislative measures to ensure that public or private parties do not unduly interfere with such right. The data protection instruments introduce procedural duties for data controllers. Data should only be processed for legitimate and clearly enumerated purposes, in line with the principles on data quality, security, information to be given to data subjects and transfers. Moreover, all instruments entitle the data subjects with procedural rights to control the dissemination of their personal information. Furthermore, Convention 108 introduced the norm, codified in article 8 EUCFR, of independent oversight, entrusted to a data protection authority.

Limitations. In all instruments, the right to privacy is not an absolute right. In other words, it can be interfered with by means of permissible limitations, which must respect a number of criteria that have been interpreted and clarified by case law. Limitations must be provided for by the law of the member state (principle of legality), be non-arbitrary, and adopted for explicit purposes 'necessary for the protection of fundamental values in a democratic society', such as for reasons of state security, public safety, monetary interest of the state, suppression of criminal offences,

protection of the data subject, or protection of the rights and freedoms of others. A more nuanced test for permissible limitations is presented in the deliverable.

Recent legislation in the field of AFSJ regulating the use of personal data (section 2.2)

The review conducted on recently adopted legal instruments disciplining the use of personal data for police and judicial cooperation seems to confirm the reality of the security vs. privacy trend. The Council Framework Decision 2008/977/JHA provides a clear example. Firstly, the Framework Decision has a limited scope, as its provisions do not apply to domestic situations. Secondly, its articles 3.2, 11 and 12.2, taken together, provide for a blanket exception to the purpose limitation principle. Thirdly, article 13 allows member states to transfer personal data received from another member state to either third states or international bodies without strict safeguards. Another departure from the purpose limitation principle is the increasing use by national LEAs and relevant EU agencies, such as Europol and Eurojust, of personal data stored in EU databases that were not exclusively set up for law enforcement purposes, such as Eurodac and the Visa Information system (VIS).

The general trend, whereby LEAs increasingly access data of individuals, who, in principle, are not suspected of committing any crime, informs also the Data Retention Directive. According to the Article 29 Data Protection Working Party and the EDPS, its permissible limitations are insufficient. The data retained shall be provided to (1) the competent national authorities, (2) in specific cases, (3) for the purpose of the investigation, detection and prosecution of serious crime, as defined by each member state in its national law. The Data Retention Directive does not provide any further details on the procedures to be followed and the conditions to be fulfilled in order to gain access to retained data, which leaves room for heterogeneous interpretations in the acts transposing the directive into national law. Indeed, an evaluation by the Commission showed that "[M]ost transposing Member States, in accordance with their legislation, allow the access and use of retained data for purposes going beyond those covered by the Directive, including preventing and combating crime generally and the risk of life and limb".

Comparative review and analysis of recent judgments appraising the permissible limitations to privacy in AFS policies (section 3)

This deliverable analyses the interpretation of permissible limitations by three judicial (or quasi-judicial) bodies – the HRC, the ECtHR and the ECJ – in the context of security related case law, in particular where security and privacy were weighed as competing interests, or the problem was avoided altogether.

On the one hand, the HRC, the ECtHR and the ECJ have consistently, and overtly, avoided to provide strict definitions of the rights to privacy and data protection, thus leaving open the possibility to extend its scope of application to new technologies. However, such an approach has hindered to achieve a definition of what constitutes the essence of the rights to privacy and data protection, which weakens the imposition of clear and strict permissible limitations existing in leges generales, and the many leges speciales recently adopted to overseeing the use of SOSTs.

On the other hand, the three judicial bodies seem to have progressively refined the scope of application of limitations and the principles regulating their implementations in response to technological and procedural advances, although the scope of application is not always clear.

The European Court of Human Rights has progressively refined the parameters that national legal legislation should respect. However, it has never addressed the right to privacy in terms of a core and, in certain instances, it has granted a generous margin of appreciation to states to restrict this right.

As for the Court of Justice of the European Union, its limited jurisdiction over fundamental rights meant that, before the entry into force of the Lisbon treaty, it avoided the problem altogether, as demonstrated by the PNR and Data Retention cases. Since Kadi (I), though, the Court may be seen to have taken a bolder approach, in line with its recently acquired competence in deciding on matters of fundamental rights without any review of their impact on the internal market.

So far, the strictest application of the test for permissible limitations seems to have been applied by national constitutional courts, as the case of data retention appears to demonstrate.

Core/periphery as a constructive approach towards the acceptability of technology (section 4)

The deliverable suggests an analytical alternative to the security vs. privacy approach, namely the core/periphery approach based on a reinterpretation of Alexy's theory of rights. Accordingly, all human rights or fundamental rights would have an inviolable core sealed in a rule, and a periphery surrounding that core and subject to permissible limitations, such as those foreseen by article 8 ECHR, and articles 7 and 8 of the EUCFR, for privacy and data protection. Such a core/periphery approach to rights, reflected in EUCFR article 52(1), lays the basis for combining compliance with the rights to privacy and data protection and the needs of LEAs when conducting an investigation or addressing in a more general fashion privacy and security, as opposed to simple theories of abstract balancing. The latter easily result in a choice between the two, and usually in always prioritizing security, hence eroding privacy to an empty shell.

Three different criteria have been preliminary identified as candidates to determine the scope of the core of the right to privacy: sensitive data as privileged content, information produced in the course of confidential personal relationships, and methods of intrusion. The inviolability of the essential core of any human right – in this case the right to privacy – is one of the steps in an analytically rigorous test for the permissibility of restrictions, whereby all of the following cumulative conditions must be met: (a) any restrictions must be provided by the law; (b) the essence of privacy/data protection is not subject to restrictions; (c) restrictions must be necessary in a democratic society; (d) any discretion exercised when implementing the restrictions must not be unfettered; (e) for a restriction to be permissible, it is not enough that it serves one of the enumerated legitimate aims; it must be necessary for reaching the legitimate aim; (f) restrictive measures must conform to the principle of proportionality, they must be appropriate to achieve their protective function, they must be the least intrusive instrument amongst those which might achieve the desired result, and they must be proportionate to the interest to be protected; and (g) any restrictions must be consistent with other human or fundamental rights.

The test could also be interpreted as an instrument to determine the acceptability of the use of new technologies, whenever an interference with the right to privacy is the outcome.

Application of the core/periphery approach to selected technologies (section 5)

Section 5 of the deliverable applies the test to four relatively new technologies: GPS-based location trackers, smart CCTV, network surveillance by means of deep-packet inspection engines and surveillance by means of Trojan Horses.

GPS-based location trackers allow the continuous monitoring of the location of any object equipped with a GPS receiver anywhere on earth. A core/periphery theory of rights would therefore suggest that only investigations into the most serious offences would justify the combination of GPS data with other datasets. In practice, however, it seems unclear how a judge would be able to prevent law enforcement officials from entering a specific location in a tool such as Google Maps in order to get more information about certain facilities that are nearby a suspect's location.

Smart CCTV cameras add new hardware and software capabilities to CCTV cameras in order to enable the automated recognition of 'unusual' or 'interesting' predetermined traits, risk factors or situations, which in turn would enable a CCTV-operator to prevent such a situation from happening. A key feature of smart surveillance technologies is that they are used to monitor identifiable persons as they are moving in publicly accessible places. In theory, smart surveillance could be seen as a 'privacy-proof' way of conducting surveillance only in relation to persons suspected of a crime. The greatest concerns relating to the use of smart surveillance cameras are the underlying definitions of what constitutes an 'abnormal' or 'unusual' behaviour that a smart CCTV camera should recognize and monitor. There exists a risk that the use of certain indicators may amount to discrimination, by singling out individuals or social groups for adverse treatment on the basis of incorrect or misleading assumptions. If smart surveillance measures want to be compliant with the ECHR, it is clear that they must be based on a particularly precise domestic law, which has to give citizens an adequate indication of the conditions and circumstances in which the authorities are empowered to resort to such measures.

Deep-Packet Inspection (DPI) implemented by ISPs is a technology capable of extracting user data sent over the networks. It applies to information flows and allows a full analysis of such data,

thanks to its capability of inspecting each layer of the Open Systems Interconnection (OSI) model, i.e. the header and the payload (i.e. content) of the data packets, including the application layer, which contains the most confidential user data (what is commonly referred to as the content of communications). DPI could violate the prohibition of processing sensitive data enshrined in article 8 of Directive 95/46/EC, and as such could violate one potential element of the core identified in section 4. DPI infringes data protection principles such as openness (the system is secret) and individual participation (users cannot oppose the processing). As such it is always used without the knowledge of the user, which makes it a more intrusive technology to the core of the right to privacy. Since the integrity of the gathered data cannot be verified and unlimited information can be easily accessed and used for a wide variety of purposes, DPI is very hard to square with key data protection principles such as data quality, collection limitation and purpose specification (if the extra data collected leads to further uses than the one initially envisaged). Finally, but crucially, it can breach the prohibition of automated individual decisions enshrined in article 15 of Directive 95/46/EC. The use of DPI by ISPs tout court, and for security purposes (i.e. child pornography), is highly unlikely to pass the very first part of the permissible limitation test, namely the principle of legality.

A **Trojan Horse** is a program, i.e. a string of code, that creates a backdoor in a computer. The applications range from stealing and deleting data (proper computer crimes), to the point of completely taking over the machine of the user, to monitoring legitimate users, aka governmental surveillance, which is the application of our interest here. Surveillance by Trojans may look advantageous as opposed to generic DPI, in that it is 'targeted' or 'smart', similarly to the case of smart CCTV. Whereas it does not treat all citizens as potential suspects, Trojans can nonetheless be highly intrusive for its monitoring capability. The impact on the rights to privacy and data protection is similar to generic DPI; the difference is that the security safeguards principle (as regards the device of the monitored individual) is by definition violated. The use of Trojans can be allowed only if done in strict accordance with the permissible limitation test.

Interdependencies

This paper is part of the SurPRISE project. The ultimate objective of this deliverable is, therefore, to provide an academic legal underpinning for the multi-national participatory large-scale events wherein citizens' views on security and privacy will be thoroughly assessed (work packages 5 and 7). Accordingly, it interacts with the results of work package 2, which assesses surveillance-oriented security solutions; it provides the basis for work package 4 on a questionnaire and information material and, later on in the project, work package 6 on analysis and synthesis.

More immediately, it dialogues with, and builds upon, the other pieces of work produced in Work Package 3 ("exploring the challenges"), which "addresses the problems of privacy and security from an acceptability perspective investigating in detail technological developments and their legal governance against the background of alternative (e.g. non-technical) options for handling security threats". In particular, the analysis of the permissible limitations in the use of new technologies builds upon the technical analysis formulated within the 'Report on surveillance technology and privacy enhancing design' (Deliverable 3.1).

1. Introduction[1]

The aim of this deliverable is to review "the current state, and explore challenges and options for political and legal developments, on privacy and security"[2] in the European Union (hereafter EU), which are two evolving and contested concepts. This review will pursue two intertwined objectives. Firstly, we will carry out a legal analysis of the deployment of security technologies featuring surveillance capabilities, a.k.a. surveillance-oriented security technologies (hereafter SOSTs), and the policies behind the adoption of such SOSTs (a.k.a. surveillance-oriented security solutions, hereafter SOSSs). Secondly, we will scrutiny the legal dimensions of the so-called 'security vs. privacy' trade-off inherent in many of such policies, whereby security and rights are presumed irreconcilable interests, and security easily trumps rights due to its purported overarching societal weight.

The deliverable provides a detailed comparative review and analysis of recent judgments and legislation in the field of privacy and security, in order to achieve three immediate objectives. Firstly, capturing the legal norm of the fundamental right to privacy (and, where appropriate, the legal norm of the fundamental right to the protection of personal data); secondly, determining the legal permissibility of restrictions applied to this right; and finally, reflecting upon European judgments in which the right to privacy was 'balanced' with the need to provide security.

The test for permissible limitations to the right to privacy (and its neighbouring right of data protection), combined with the elaboration of a 'core/periphery' structure of such rights, may provide a framework for evaluating the legal acceptability of the deployment of SOSTs and SOSSs in the European Union. To this end, the deliverable investigates the permissible limitations relating to the use of the following security technologies and practices: GPS-based location trackers, smart close-circuit television cameras (hereafter CCTV), deep-packet inspection for network surveillance, and Trojan Horses used for single device surveillance purposes.

1.1 Interdependencies within the SurPRISE project

This paper is part of the SurPRISE project, which stands for "Surveillance, Privacy and Security: A large scale participatory assessment of criteria and factors determining acceptability and acceptance of security technologies in Europe." The ultimate objective of this deliverable is, therefore, to provide an academic legal underpinning for the multi-national participatory large-scale events wherein citizens' views on security and privacy will be thoroughly assessed (work packages 5 and 7). Accordingly, it interacts with the results of work package 2, which assesses surveillance-oriented security solutions; it provides, together with other work in work package 3, the basis for work package 4 on a questionnaire and information material and, later on in the project, work package 6 on analysis and synthesis.

More immediately, it dialogues with, and builds upon, the other pieces of work produced in work package 3 ("exploring the challenges"), which "addresses the problems of privacy and security from a broader acceptability perspective investigating in detail technological developments and their governance (including legal regulation) against the background of alternative (e.g. non-technical) options for handling security threats".[3] In particular, the analysis of the permissible limitations in the use of new technologies will build upon the technical analysis formulated within the 'Report on surveillance technology and privacy enhancing design' (Deliverable 3.1).

---

[1] The authors would like to thank the many contributors who have made the successful completion of this deliverable possible: Javier Sempere Samaniego (former APDCM) and Stefan Strauß (ITA) for the provision of material for the national data retention case law, and cyber surveillance, respectively; Johann Cas, Walter Peissl (ITA), and Ben Wagner (EUI) for their invaluable comments on the technology sections; Jonathan Andrew (EUI) for the prompt linguistic revision; Javier Sempere Samaniego (former APDCM), Monica Arenas Ramiro (UdA) and Colin Bennett (VUB, UoV) for comments on the legal analysis and the papers' structure; the participants of the experts workshop held in Vienna on February 12th, 2013 for insights and suggestions; and all the SurPRISE consortium partners who reviewed the deliverable during its development and supported our work.

[2] SurPRISE Project Consortium (2011), part A, p. 13.

[3] SurPRISE Project Consortium (2011), part A, p. 13.

1.2 Research approach, methodology and definitions

This paper is based on both primary and secondary sources. The primary sources used consist mainly of EU treaties, legislation and case law, and on international (human rights) treaties, insofar as they are applicable to the EU and its member states, as well as on national and international case law, with a view to carrying out the comparative analysis. Secondary sources consist mainly of technical sources relating to the four technologies analysed (beyond the results of the Report on surveillance technology and privacy enhancing design) on the one hand, and on legal scholarship/literature on the theory of rights, the contested notions of privacy and security, and their relationship in the context of SOSTs and SOSSs on the other.

In line with the objectives of the SurPRISE project, this deliverable will challenge the assumption that the collective interest to, or public good of, security and the rights to privacy (and data protection) are irreconcilable in the EU. In fact, after the terrorist attacks of 9/11, the already existing trend towards intelligence-led policing, i.e. law enforcement activities driven by the collection of personal information, has exponentially increased, leading to the routine use of surveillance (SOSTs and SOSSs). In the security context, surveillance comprises the targeted or systematic monitoring, by governmental organizations and their partners, of persons, places, items, infrastructures or flows of information, in order to identify hazards and manage risks and to enable, typically, a preventive, protective or reactive response, or the collection of data for preparing such a response in the future.[4] The ensuing policies framed the relationship between privacy (together with data protection) and security predominantly in terms of the need to 'strike a balance' or establish a 'trade-off' between security and rights. The ensuing restrictions imposed on the two fundamental rights for the purpose of security have arguably exceeded the permissible scope of limitations to both rights so that it can be questioned whether all resulting limitations are actually compatible with the values these rights seek to protect.[5]

This should not be the outcome.[6] In fact, pursuant to article 2 of the Treaty on European Union (hereafter TEU)[7], the EU is "founded on the values of respect for human dignity, freedom, democracy, equality, the rule of law and respect for human rights." Human rights encompass privacy and data protection, enshrined in articles 7 and 8 of the European Charter of Fundamental Rights (hereafter EUCFR) respectively, which enjoys a status analogous to constitutional Bills of Rights in nation states[8] and which established clear rules for permissible limitations.[9] Furthermore, human rights constitute "general principles' of the Union's law" (TEU article 6.3), whereof the Court ensures observance,[10] at a minimum "as guaranteed by the European Convention for the Protection of Human Rights and Fundamental Freedoms and as they result from the constitutional traditions common to the Member States" (TEU article 6.3).[11] Disrespect of human rights can trigger the procedure of serious breach by a Member State, introduced by TEU article 7. As recognized by the Court of Justice of the European Union in *Wachauf*:

> *"The fundamental rights recognized by the Court are not absolute, however, but must be considered in relation to their social function. Consequently, restrictions may be imposed on the exercise of those rights (…) provided that those restrictions in fact correspond to objectives of general interest pursued by the Community and do not constitute, with regard to the aim pursued, a disproportionate and intolerable interference, impairing the very substance of those rights."*[12]

---

4 This definition of surveillance is based on the (SURVEILLE Project Consortium, 2011), p. 46, as modified for the purposes of SURPRISE.
5 Scheinin (2009a). For a complete analysis of the costs of surveillance, see (IRISS Project Consortium, 2012).
6 Buttarelli (2011b).
7 "Consolidated versions of the Treaty on European Union (TEU) and the Treaty on the Functioning of the European Union (TFEU)."
8 Article 6.1 TEU.
9 That is, article 52 TEU, which will be analysed in details in Section 2.
10 C-4/73, "Nold KG v Commission" (1974), paragraph 13.
11 Craig and de Bùrca (2011).
12 C-5/88, "Wachauf V Bundesamt Für Ernährung Und Forstwirtschaft" (1989), emphasis added.

Objectives of general interest, or aims, pursued by the EU are "the promotion of peace, the preservation of its traditions and citizens' well-being."[13] This translates, first and foremost,[14] into the creation of an internal, borderless area, protecting citizens' fundamental rights, guaranteeing a high level of security and fostering access to justice, in respect of the different legal systems and traditions proper of member states: the Area of Freedom, Security and Justice (hereafter AFSJ).[15] The AFSJ substitutes the former "third pillar", or area of police and judicial cooperation governed by intergovernmentalism[16] and, pursuant to article 4.2 (j) of the Treaty on the Functioning of the European Union (hereafter TFEU)[17], is now an area of shared competence between the EU and the Member States.[18] Hence, the AFSJ falls within the scope of EU law and is subject to the authority of the Court of Justice of the European Union laid down by article 19 TEU.[19]

The EU's political priority, as expressed in the five-yearly programmatic document for the AFSJ, is to "ensure respect for fundamental freedoms and integrity while guaranteeing security".[20] At the same time, the underlying value of 'security' is the promotion of "human rights, democracy, peace and stability."[21] In other words, security is instrumental to the pursuit of a society wherein human rights, including privacy and data protection, are fully enjoyed. While ECHR article 5 and ICCPR article 9 refer to 'security of the person' as an individual right, the relationship between privacy and security is usually not formulated as a tension between two competing individual human (or fundamental) rights, but as a question of how far the collective goal of public security can constitute a legitimate aim that justifies permissible limitations to the individual right to privacy, or data protection. That is a meaningful question that can be addressed through legal analysis.

A part of the problem relating to the 'security vs. privacy' debate lies in the contested nature of the concepts under analysis. 'Security' is vaguely referred to in the TEU in articles 3.2 and 3.5, 21.2 (a) and (c). AFSJ-related policy documents describe it through risks, or threats "which have a direct impact on the lives, safety, and well-being of citizens."[22] Threats are usually grouped in broad categories, which inform the basis of policy making in the AFSJ (under the impetus of "the strategic guidelines for legislative and operational planning" identified by the European Council as laid down in article 68 TFEU), and include "serious and organised crime, terrorism, drugs, trafficking in human beings and smuggling of persons"[23] as well as "cybercrime, the management of…external borders and…natural and man-made disasters."[24] Article 83.2 TFEU on judicial cooperation identifies the following "areas of particularly serious crimes with a cross-border dimension (…): terrorism, trafficking in human beings and sexual exploitation of women and children, illicit drug trafficking, illicit arms trafficking, money laundering, corruption, counterfeiting of means of payment, computer crime and organised crime," without contextualizing security any further.

The vagueness of the concept coupled with the emotional thrust for strong responses in the wake of security failures, such as terrorist attacks, have led to the adoption of policies based on the extensive processing of personal information, which claim to 'strike a balance', i.e. weigh fairly security interests and privacy (and data protection) rights, but de facto result in introducing

---

13 Article 3 TEU.
14 Craig and de Bùrca (2011).
15 Article 3.2 TEU, article 67 of the Treaty on the Functioning of the European Union.
16 However, the so-called *passerelle*, now enshrined in article 48(7) TEU, had led to the 'communitarization', i.e. the use of the communitarian method (whereby the Commission has the power of initiative), for some matters falling in the area of police and judicial cooperation in the Treaty of Amsterdam.
17 "Consolidated versions of the Treaty on European Union (TEU) and the Treaty on the Functioning of the European Union (TFEU)."
18 This is an area subject to the 'pre-emption' clause, whereby member states can "exercise their competence to the extent that the Union has not exercised its competence" (article 2TFEU, paragraph 2), which will necessarily affect the exercise of the exclusive competence of Member States in the maintenance of law and order and the safeguarding of internal security (article 72 TFEU) (Craig and de Bùrca, 2011).
19 Subject to the rules of Protocol 36, as addressed in section 3.4.
20 Council, 2010b, p. 4.
21 Council, 2010b, p. 4.
22 Council 2010a, p. 3.
23 Council 2010a, p. 35.
24 European Commission (2010e), p. 2.

excessive limitations to such rights. Moreover, the inherent value of privacy and data protection has been contextually challenged. This deliverable intends to demonstrate that privacy and data protection are not empty concepts, and to show their continued significance in our society.

1.3 Outline

This deliverable is divided into four parts. Section 2 contains a review and analysis of key general legislation in the area of privacy and data protection, as well as recent legislation in the field of privacy and security, both in the AFSJ and the so-called 'external area of the AFSJ', which identifies legally permissible restrictions applicable to privacy and data protection. Section 3 contains a comparative analysis of recent judgements relating to security and privacy/data protection, which allows reflecting upon European judgments in which the right to privacy was 'balanced' with the need to provide security. Section 4 addresses the norm of the fundamental right to privacy through a 'core/periphery' analysis. Section 5 demonstrates how such an analysis can guide the deployment and use of a number of relatively new technologies, including GPS-based location trackers, smart CCTV, network surveillance by means of deep-packet inspection, and device surveillance by means of Trojan Horses. Finally, the conclusions summarize the discussions and provide suggestions for deliverable 3.4 'Synthesis paper on comprehensive security enhancing policy options', which will translate the theoretical results of this and other WP3 deliverables into topics of discussion for the sake of the multi-national large-scale participatory citizens' events.

2. Legislative development of the right to privacy and its limitations

This section addresses the "evolving and contested concepts of privacy and security"[25] in European Union legislation, in order to lay the basis for (i) precisely capturing the norm of the fundamental right to privacy (see *infra* 2.1) and (ii) determining what kinds of restrictions (or limitations) upon this fundamental right are legally permissible (see *infra* 2.1 to 2.3). To this end, it provides a short overview of the legislative evolution of the right to privacy, and of the related right of data protection, and then focuses on these two fundamental rights in the AFSJ, and the external area of AFSJ.

The first enshrinement of privacy as a right in a (international) legal instrument, namely the Universal Declaration of Human Rights (hereafter UDHR), was the result of a legal discussion that started at least 50 years earlier. Indeed, the right was legally formulated for the first time in the United States in a seminal article written by Warren and Brandeis.[26] The right was quickly labelled as 'the right to be let alone,"[27] but the authors articulated it further. Firstly, privacy was described as embodying the need to legally protect an emerging societal, moral and philosophical need, "a right to personality" or identity, namely the expressions of one's life, such as emotions, sentiments, facts of life, happenings, actions, sexual life and relationships with others. Secondly, the formulation of such a right would counter unpredictable negative effects of technological evolutions (such as – at that time – the improvement of photography allowing taking pictures at a distance) and related consequences (i.e. the proliferation of sensational periodicals publishing unwanted pictures).[28]

These are two defining elements of the right to privacy that may be seen as informing its further legal development. On the one hand, privacy "refers to the sphere of a person's life in which he or she can freely express his or her identity, be it by entering into a relationship with others, or alone."[29] Such a private sphere allows "individuals and groups to be able to think and develop ideas and relationships".[30] It is based on the libertarian idea of autonomy and freedom of action,[31] manifested in the private sphere as individuals free from the State's interference (home, body and correspondence), and in the public sphere as citizens,[32] which seems to belong in different forms to all cultures,[33] and is indeed included in most constitutions.[34] Some authors refer to privacy as a meta-right, serving as the basis for civil and political rights such as freedom of expression, association, and movement, which could not be effectively enjoyed otherwise.[35] On the other hand, privacy puts normative limits to technological advances and related practices, which enhance human possibilities in either sense, and in particular interfere with autonomy and freedom (home, body and correspondence). The internationalization of privacy threats allowed by trans-border data flows (see *infra* 2.1.2) further informed its legal development. We shall now turn to the legal instruments embodying privacy applicable in the European Union, which we propose to read in a holistic manner.

---

25 SurPRISE Project Consortium (2011), part A, p. 13.
26 Warren and Brandeis (1890).
27 The formulation was borrowed, in turn, from a formulation of Judge Cooley (id.).
28 Id.
29 A.R. Coeriel et al. v. the Netherlands, 453/91, p. 79 in Blair (2005).
30 Scheinin (2009a), p. 13.
31 Rehof (1992; 1995).
32 Nowak (2005).
33 Westin (1967).
34 Drafting Committee on an International Bill of Human Rights (1947).
35 Rodotà (2009); Scheinin (2009a).

2.1 A concise overview of the evolution of the rights to privacy and data protection and their limitations

2.1.1 The foundations of the right to privacy: the UN Universal Declaration of Human Rights, the European Convention on Human Rights and the International Covenant on Civil and Political Rights

Article 12 UDHR, article 8 of the Council of Europe's Convention for the Protection of Human Rights and Fundamental Freedoms (a.k.a. European Convention on Human Rights, hereafter ECHR) and article 17 of the United Nation's International Covenant on Civil and Political Rights (hereafter ICCPR), are the first instruments enshrining the right to privacy. In spite of the prudence exercised by the Court of Justice of the European Union in referring to international legal instruments beyond the ECHR,[36] it could be argued that these three foundational documents should be read together with a view to understanding the essence of the right to privacy in the EU.

In fact, the formulation of article 3.5 TEU, the explanatory rules to the EUCFR (which refer to the international human rights legal framework and acknowledge the interconnectedness of various sources),[37] and legal scholars/jurisprudence[38] generally suggest that fundamental rights in the EU should be interpreted in light of the existing international legal instruments to which Member States are party. Such an interpretation would make sense to better understand the scope of the right to privacy in the EU, since article 12 UDHR lays the foundations for both article 8 ECHR[39] and article 17 ICCPR.[40] Both rights are underpinned by the same motivations, bear similar scope and meaning, and are enshrined in instruments that are legally binding for the Member States.[41]

Motivations. The underlying motivation for the adoption of article 12 UDHR[42] was the reestablishment of universal dignity (which encompasses autonomy) and freedom,[43] which were heavily affected by the atrocities of WWII.[44] The adoption of article 8 ECHR was similarly justified on grounds of the horrors of the exercise of totalitarian power. The ECHR Drafting Committee

---

36 European Court of Justice, Opinion 2/94, (1996), paragraph 33. The Court of Justice is reluctant to acknowledge the relevance of international instruments that are sources of human rights in interpreting the fundamental rights in the EU, with the exception of the ECHR, which holds "a special significance" for the interpretation of the general principles of the EU (European Court of Justice, Opinion 2/94, 1996, ECR I-1795, paragraph 33). See for instance *Kadi I*: "the Court draws inspiration from (…) the guidelines supplied by international instruments for the protection of human rights on which the Member States have collaborated or to which they are signatories ("Kadi I," 2008, paragraph 283).

37 This is the case, for instance, of article 1 on human dignity, derived form the Universal Declaration of Human Rights (European Parliament, 2007; European Union Network Of Independent Experts On Fundamental Rights, 2006).

38 European Union Network Of Independent Experts On Fundamental Rights (2006).

39 The travaux préparatoires of article 8 testify to such connection with article 12 UDHR; the first voted version of the article included the expression "as laid down in article 12 of the Declaration on Human Rights of the United Nations" (European Commission of Human Rights, 1956). Moreover, the doctrine interprets the copious case law relating to article 8 as a legally binding elaboration of the principles enshrined in article 12 (Rehof, 1995). As for article 17 ICCPR, it had not been proposed yet at the time of the voting on article 8, although the Committee of Experts on Human Rights pointed out that "due attention should be paid to the progress which had been achieved in this matter by the competent organs of the United Nations" (European Commission of Human Rights, 1956, p. 4).

40 The travaux préparatoires of article 17 of the International Covenant on Civil and Political rights also highlight a direct line with article 12 UDHR, whereas there is no direct connection with article 8 ECHR, but in any case they are linked (see note *supra*).

41 The UDHR was adopted by means of a resolution of the General Assembly, which is not legally binding as a document. However, it has been argued that the Declaration, or part of it, has acquired the character of customary law, and as such is legally binding, due to whole or partial incorporation in national constitutions, being referred to in several judgements and informing international conventions (Krause and Scheinin, 2009).

42 Morsink (1999).

43 Which is enshrined in article 1.

44 In the language of the UDHR, these are "barbarous acts which have outraged the conscience of mankind", such as the intelligence-led (i.e. linked to census and data mining) extermination of the Jewish population and other enemies by the Nazi (Arendt, 2011).

envisaged article 8 to protect persons against racially segregated marriage and the regimentation of children and young persons, which were two practices conducted by the totalitarian regimes.[45]

Converging meaning. UDHR article 12,[46] modelled on the 4th amendment to the US Constitution,[47] contains both a duty to respect and to protect by the state. Its formulation protects the development of one's personality (privacy, honour and reputation), including personal relationships and all intermediary elements (family, home and correspondence), and as such must be read in conjunction with articles 10, 11 (habeas corpus and due process), 17.2 (deprivation of the place of habitation) and 18-19 (freedom of thought, conscience and opinion).[48]

Article 8[49] ECHR protects the 'respect' of private life, which is generally seen to include the right to a name, physical integrity (including body searches),[50] collective health protection, home, correspondence (which includes all forms of communications), processing of personal data, sexual life, telephone calls;[51] family life (which includes family in a wide sense, parent-child relationship, immigration and expulsion, minors entrusted to other families).[52] The Court's interpretation has evolved, thus leading to an ever-expanding inclusion of situations deserving respect. Yet, the Court has focussed more on the meaning of the interferences, thus interpreting article 8 *a contrario*, in the light of its clearly enumerated limitations.[53]

Article 17 ICCPR[54] is to date the geographically most widely endorsed provision on privacy;[55] however, it expresses a general rule, which can be adapted by the state parties.[56] Albeit modelled on article 12 UDHR, its elements are subject to a wide range of interpretations. Privacy includes identity, integrity and intimacy, relating to the body, acts and information, and autonomy of action;[57] family is broadly interpreted and understood as in the state party at stake;[58] home is the place where one resides or works;[59] correspondence extends beyond letters. Honour and reputation are not defined, but are still protected from attack.

Restrictions/ Permissible limitations. The combined reading of articles 12 and 29 UDHR, article 8.2 ECHR and articles 17 and 4 ICCPR, the latter in conjunction with General Comment 16 and the Human Rights Committee's jurisprudence,[60] demonstrate that the right to privacy is not an absolute right; it can be interfered with by means of permissible limitations. In order to qualify as permissible, interferences or attacks must be: lawful, i.e. conform to the laws of one's country and international obligations (articles 12 UDHR, 8 ECHR and 17 ICCPR); non arbitrary, i.e. reasonable and in line with "well-established legal principles" (articles 12 UDHR and 17 ICCPR); "necessary in a democratic society" (article 8 ECHR); carried out for explicit purposes (article 29 UDHR, 8.2 ECHR and 4 ICCPR). All instruments clarify that the State is under the legal obligation

---

45 European Commission of Human Rights (1956), p. 4.

46 Under article 12 UDHR, "*no one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks".*

47 Morsink (1999).

48 Rehof (1992).

49 Under article 8 ECHR (Right to respect for private and family life), "1. Everyone has the right to respect for his private and family life, his home and his correspondence. 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others".

50 Rehof (1992).

51 Zencovich (2001).

52 Id.

53 Id.

54 Under article 17 ICCPR: (1) No one shall be subjected to arbitrary or *unlawful* interference with his privacy, family, home or correspondence, nor to *unlawful* attacks to their honour *or* reputation. (2) Everyone has the right to the protection of the law against such interference or attacks.

55 Scheinin, 2009a. 167 of states are parties to the Convention, available at: http://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtdsg_no=IV-4&chapter=4&lang=en.

56 Nowak (2005).

57 Nowak (2005).

58 Human Rights Committee (1988).

59 Id.; Blair (2005); Nowak (2005).

60 Nowak (2005).

to refrain from unduly interfering with the right to privacy, and has positive obligations to take the necessary legislative measures to ensure that such right is not unduly interfered with by public (all articles) or private (article 12 UDHR and 17 ICCPR) parties.[61]

Divergences. It must be remembered that some differences exist among these provisions. First of all, article 8 ECHR does not encompass honour and reputation, which were deliberately scratched from the concept of privacy and inserted in article 10 instead.[62] In contrast to article 12 UDHR and article 17 ICCPR, the Convention explicitly addresses positive[63] and negative[64] interferences affecting the individual, but only when vertical, i.e. attributed to the public authority. Articles 12 UDHR and 17 ICCPR textually also address interferences that are horizontal, i.e. committed by natural and legal persons, even if also under these instruments the actual addressee is the State.

In summary, Article 12 UDHR, 8 ECHR and especially 17 ICCPR highlight the universal relevance of the right to privacy, which appears as an umbrella term[65] encompassing the protection of mental and physical (spatial and bodily) integrity, intimate relationships,[66] and information relating to such spheres, often grouped into four categories of privacy: bodily, relational, informational and territorial.[67]

2.1.2 Towards a right to data protection: the OECD guidelines (FIPs) & Convention 108

The appearance of computerized systems and their applications allowed for unprecedented (personal) data processing capabilities, which opened up social, cultural and economic opportunities, including in the administration of the welfare state. A relatively small invention, the so-called 'search function,' which allowed to select the desired words or portion of content in a text, led to impressive business opportunities,[68] notably building searchable, refined databases. This in turn enabled the development of a fundamental business feature, and an additional engine for privacy regulation: the trans-border 'flows' of personal information, whereby data containing personal information were exchanged, point-to-point, to supply national and international businesses (shipping, travelling) or as a business itself (i.e. for marketing).

Such developments triggered comprehensive academic and legal reflections on the possible impact on human rights, the establishments of international thematic commissions producing reports and studies, as well as international declarations, such as the UN 1975 Declaration.[69] The object of these studies focused on a particular aspect of privacy, namely the protection of personal information contained in electronic, machine-readable data, which paved the way to the progressive acknowledgement of the right to data protection.

Partly prompted by the uncovering of information-surveillance related scandals, such as the Watergate, Safari and Fiat scandals in the US, France, and Italy, several countries started tackling the challenges posed by data processing.[70] One major study conducted in the US by the

---

61 As for honour and reputation, the burden of proof of the unlawfulness is on the plaintiff, in order to safeguard the potentially competing right of freedom of expression (Simons v. Panama 460/91 and I.P. v. Finland 450/91; 380/89 in Blair (2005).

62 European Commission of Human Rights (1956).

63 Meaning actions.

64 Meaning inactions.

65 Nowak (2005); Rehof (1995).

66 Rehof (1995).

67 Electronic Privacy Information Centre (EPIC), 2006. But "Since Clarke's conceptualisation, new and emerging technologies have introduced further privacy effects, and Clarke's four categories are no longer adequate to address the concerns they introduce. Our seven types of privacy include privacy of the person, privacy of behaviour and action, privacy of personal communication, privacy of data and image, privacy of thoughts and feelings, privacy of location and space and privacy of association (including group privacy)" (Finn et al., 2013).

68 Eriksson and Giacomello (2012); Sartor (2010).

69 United Nations (1975).

70 See, for instance, Younger, (1972). Notably, the Land of Hesse adopted a "Data Protection Act" in 1970, which was more concerned with the public sector data practices (The German Tribune, 1973). Sweden was the first country to adopt a "Data law" in 1973, recommended by a study on automated data

Advisory Committee on Automated Personal Data Systems (1973), relating to automated data systems in the public administration, led to the formulation and recommendation for adoption of 'standards' to treat such data fairly to avoid any possible unwelcome effects. The so-called Fair Information Principles (hereafter FIPs) introduced eight tenets: openness (prohibition of secrecy); individual access (to one's own personal data); individual participation (correction and amendment); collection limitation (by one organization); use limitation (by one organization); disclosure limitation (to external organizations); information management (necessity, lawfulness, accuracy); and accountability (record keeping).

> Firstly applied in the US in the 1974 Privacy Act and further refined in 1977,[71] FIPs were destined to be extremely successful,[72] as they informed the discussions and rules adopted at the international level to address the protection of (trans-border) processing and flows of personal data, notably the Privacy Guidelines[73] of the Organization for Economic Cooperation and Development (hereafter OECD) and Convention 108[74] of the Council of Europe. For the OECD – which groups the "most advanced countries and emerging ones"[75]– in line with its tasks of economic growth enshrined in article 1 of the Convention,[76] the most pressing need in the adoption of the Privacy Guidelines was to allow the smooth trans-border flow of personal data, while the protection of privacy, although recognized by all member countries, was seen as secondary.[77] The Guidelines apply to data processing carried out by both automatic and manual means, and by both the private and public sectors. The Guidelines incorporated and adapted, for the first time in an international legal (although entirely voluntary) instrument, the FIPs, which it dubbed 'principles'. These are: collection limitation; data quality (ca. FIP information management); purpose specification (ca. FIP use limitation); use limitation (ca. FIP disclosure limitation); security safeguards (ca. FIP information management); openness; individual participation; and accountability.[78]

The OECD's formulation of FIPs has been very influential in the parallel drafting of Convention 108.[79] In keeping with the values of the Council of Europe, which gathers European states committed to the advancement of democracy and the rule of law, the primary objective of Convention 108 was protecting everyone's right to privacy.[80] Promoting the freedom of information across borders came only as a secondary goal. The Convention, which applies to any information relating to an identified or identifiable individual (personal data) processed wholly or partly by automatic means[81], both by public and private parties[82], gives substance to the OECD principles in a legally binding manner in its Chapter II (the central part of the Convention). Article 5

---

processing, following public outcry after the decision to automatize the census (Swedish Justice Department, 1972) (Newman, 2008; Rodotà, 1973).

71 Gellman, 2012.

72 However, as Gellman put it, "FIPs may have become a form of generic trademark for privacy principles rather than an indicator of any affiliation with the original standards." Gellman (2012), pp. 17-18).

73 Organization for the Economic Cooperation and Development, 1980.

74 "Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data," 1981.

75 See at: http://www.oecd.org/about/membersandpartners/.

76 See at: http://www.oecd.org/general/conventionontheorganisationforeconomicco-operationanddevelopment.htm.

77 Preamble, Organization for the Economic Cooperation and Development, 1980.

78 The OECD has since then acted as a forum of discussion for a number of issues, such as the cross-border enforcement of privacy laws (quote the recommendation) and the demand for standards to ensure the security of personal data as part of a wider cyber-security strategy (quote the recommendation). Thus, it acted as an arena to confront opposing views, particularly those of the US and the EU, and to understand them. For the US, the EU's attempt to protect privacy concealed trade barriers, whereas European Community member states interpreted the US approach as a way to maintain their hegemonic position in the marketplace (Bennett and Raab, 2006).

79 "Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data," 1981, Explanatory Memorandum.

80 The European Court recognized the importance of Convention 108 in a number of cases, including in, for instance, *Rotaru v. Romania* (European Union Network Of Independent Experts On Fundamental Rights, 2006).

81 Article 1 of Convention 108.

82 Article 3 of Convention 108.

on the quality of the data encompasses the principles of collection limitation, data quality, purpose specification, and use limitation. Article 7 on data security embodies the security safeguards principle. Article 8 on additional safeguards for the data subject encompasses the principles of individual participation and openness. Whereas there is no provision on accountability, article 10 on sanctions and remedies addresses it in the negative (*a contrario)*, in that responsibility for misdeeds will be punished.

Moreover, Convention 108 proved innovative in at least two ways. Firstly, it created special categories of data, which should not be processed unless specific safeguards apply.[83] These are data revealing racial origin, political opinions, religious or other beliefs, health and sexual life, and data relating to criminal convictions, which are by their nature sensitive, susceptible of affecting the exercise and enjoyment of other civil and political rights. Secondly, Convention 108 proposed the idea of setting up an authority charged with the enforcement of the Convention, and thus of the rights protected therein.[84] Yet, the Convention is not self-executing, thus no directly applicable rights can be derived from it, and there is no mechanism of enforcement, thus transgressions are not subject to sanctions. States parties to the Convention were to incorporate the Convention's principles into domestic law.

The result of the process sparked by the OECD Privacy Guidelines and Convention 108[85] is twofold. On the one hand, they attempted to harmonize rules for the protection of personal information,[86] thus removing the obstacles for the free flow of personal data.[87] On the other hand, they affirmed the existence of a right to data protection safeguarding 'the digital/electronic persona' as distinct from the physical persona, needing specific legal protection, substantiated in procedural rights allowing to control the dissemination of personal information. This was reinforced not only by the copious academic literature on the subject, but also by the pivotal judgment of the German Constitutional Court in 1983,[88] which identified the right to 'informational self-determination', based on the dignity and autonomy of individuals as crucial features of citizens in a democracy.

Yet, in keeping with articles 12 UDHR, 8 ECHR and 17 ICCPR, the protection of privacy with regards to the automatic processing of any information relating to an identified or identifiable individual, was configured as a right susceptible to be limited, yet not discarded, vis-à-vis certain imperative conditions in a democratic society. Hence, despite their voluntary nature, exceptions were included in the text of the OECD Privacy Guidelines. Accordingly, permissible limitations should be as limited as possible, known to the public, and should be introduced for reasons of national sovereignty, national security and public policy (*ordre public*).[89] Likewise, article 9 of Convention 108 lays down exceptions to the basic principles of data protection, which are modelled on the limitations to article 8 ECHR.[90] Limitations must be provided for by the law of the member state (principle of legality), and 'necessary for the protection of fundamental values in a democratic society' (in the light of the conditions of each signatory party), namely enforced for reasons of state security,[91] public safety, monetary interest of the state, suppression of criminal offences, protection of the data subject, or protection of the right and freedoms of others.

---

83 Article 6 of Convention 108.

84 Article 18 of Convention 108.

85 Uruguay has recently adopted the Convention, thus being the first extra European country that adopts the Convention. In 2011 the Convention underwent a process of review: http://www.coe.int/t/dghl/standardsetting/dataprotection/modernisation_en.asp.

86 In the opinion of Bennett and Raab (2006), the OECD Guidelines were an attempt to justify self-regulatory approaches.

87 Article 12 Convention 108, and "Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and trans-border data flows," 2001.

88 "BVerfGE 65. 1 - Volkszaehlung Urteil des Ersten Senats vom 15. Dezember 1983 auf die muendlliche Verhandlung vom 18. und 19. Oktober 1983- I BvR 209.269. 362.420.440.484/83 in den Verfahren ueber die Verfassungsbeschwerden," 1983.

89 The Explanatory Memorandum to Convention 108 clarifies that the list is not exhaustive.

90 Explanatory Memorandum to Convention 108.

91 As put by the Explanatory Memorandum to Convention in the comment to article 9, "The notion of "State security" should be understood in the traditional sense of protecting national sovereignty against internal or external threats, including the protection of the international relations of the State."

The European Commission closely followed the works of Convention 108, with a view to addressing the problem of the harmonization of national laws after the Convention was drafted. The aforementioned ruling of the German Constitutional Court simply reinforced the need to adopt specific regulation protecting automatically processed information relating to identified or identifiable individuals.

2.1.3 The EU: Directive 95/46/EC, 2002/58/EC, the EUCFR and the proposed Regulation

2.1.3.1 The adoption of Directive 95/46/EC and 2002/58/EC and Regulation 2001/45/EC

As acknowledged by the European Commission, the right to privacy was not sufficiently protected in the Member States, due to the few ratifications of Convention 108, the lack of information security strategies and the divergent approaches of domestic laws. This hindered the flow of personal data, at a time when such flows became crucial for business applications, which interfered with the full realization of the internal market and affected competition.[92] Hence, the current legal framework is the result of the Commission's decision to step up the level of protection – in light of the importance of fundamental rights in the Community's legal framework, whose "action must not have the effect of reducing the level of protection but, on the contrary, of ensuring a high level of protection throughout the Community"[93] – with an internal and external integrated strategy, strongly influenced by the (former) pillars structure.

The chief instrument of this strategy is the general data protection directive, namely Directive 95/46/EC,[94] adopted on the basis of article 95 of the Treaty of the European Community, due to a lack of explicit competence of the Community in the promotion of fundamental rights. Yet, the text of the Directive acknowledges, in recital n. 10, the links with article 8 ECHR, and in recital n. 11, the links with Convention 108. The Directive could be split into four main 'building blocks'.

I. Data subjects' (vs. data controllers) informational self-determination based on the notion of personal data and protected by substantive principles. The Directive covers in article 2a the processing of "personal data," a complex term explained by four cumulative elements.[95] Firstly, personal data refers to 'information,' regardless of its degree of sensitivity, format (paper, electronic, audio) and truthfulness. Secondly, such information is 'personal' in that it must be directly and indirectly about an individual, or used for the purpose of affecting an individual, or resulting in affecting an individual. Thirdly, the person must be 'identified or identifiable' (through so-called 'identifiers'), i.e. it must be possible to distinguish such person from all other members of the group, through means (recital 26) that are likely to be used. Crucially for the purposes of this deliverable, the means are conceived of in evolutionary terms: a dynamic test should be applied to technology developments, in order to assess the potential capability of a technology to 'identify' individuals. Fourthly, the individual must be a "natural person" (data subject), that is a human living being, regardless of the residence and nationality. Legal person can still enjoy protection, subject to the decision of member states implementing the Directive (or the controller, for practical reasons).[96]

The Directive inherits the concept of sensitive data coined by Convention 108; article 8 identifies data that can only be processed within certain frameworks, in the light of the potential for discrimination that a normal processing could entail. Electronic data are protected by a *lex specialis*, Directive 2002/58/EC, analysed further below. Such conception of personal data/data subject embodies the idea of 'informational self-determination' vis-à-vis the entities deciding the purposes and means of data collection (data controllers)[97], whereby data subjects enjoy the protection of their data, whose processing is permitted subject to the principles taken from Convention 108 (and, thus, the OECD Guidelines) of lawfulness and data quality[98],

92 European Commission, 1990.
93 Id., p. 5.
94 European Parliament and Council, 1995.
95 As clarified by Article 29 Data Protection Working Party (2007).
96 Id.
97 Article 29 Data Protection Working Party, 2010a.
98 Articles 6 and 7 of Directive 95/46/EC.

transparency[99], confidentiality and security[100]. The importance of informational self-determination is fully recognized in relation to the prohibition of automated individual decisions covered by article 15, whereby legal effects significantly affecting a person cannot be produced on the sole basis of an automated processing of data, which is increasingly the case in SOSTs and SOSSs. Accordingly, data subjects enjoy substantial procedural rights, with regard to the access, correction and deletion of their data[101], supervised by national and independent Data Protection Authorities foreseen by article 28.[102]

II. Independent control. On top of the creation of national supervisory authorities the Directive created, in Article 29, the Data Protection Working Party on the protection of individuals with regards to the processing of personal data (hereafter Article 29 Working Party), tasked inter alia with the interpretation of the "questions covering the application of the national measures adopted under the Directive" with a view to its homogeneous application. The Article 29 Working Party issues Opinions, which greatly contribute to the understanding of the Directive.

III. Extraterritoriality. Given the fact that the level of protection envisaged by this architecture could be bypassed by means of data transfers to countries affording minor guarantees, the Directive foresees an "extraterritorial" mechanism to tackle such transfers. First of all, article 4 lays down the rules on territorial application.[103] The Directive applies if the controller is established on the territory of a Member State, or if it uses equipment situated in the territory of a Member State, except for transit. Any processing by a controller not falling within any of the categories established by article 4 shall respect the rules on data transfers. Article 25 permits such transfers if the recipient country allows an adequate level of protection based on substantive principles and procedural requirements of data protection, assessed in the light of all circumstances; countries having ratified Convention 108 would automatically qualify.[104] Article 26 strictly enumerates exceptions to the rule. This reflects the Commission's original external strategy, which, besides the promotion of an 'adequate level of protection' among its partners,[105] included the recommendation for a Council Decision on the accession of the European Community to Convention 108.

IV. Restrictions. In keeping with the international legal sources reviewed in the two previous sections, the right to privacy as regards to the processing of personal data is not absolute.[106] The Directive does not apply to permanently anonymous data,[107] manual, unstructured data files, data processed by controllers not established in the territory of a Member States, or using equipment located in their territories for the sole purpose of transit,[108] in the course of "household activities", and data processed outside the scope of Community law, such as in the former second (CFSP) and third (AFSJ) pillars.[109] The original strategy encompassed a draft resolution extending the application of the general directive to those areas falling outside the scope of Community law, which was only adopted as Council Framework Decision 2008/977/JHA for the third pillar (see *infra* 2.2). More fundamentally, article 13 of the Directive allows Member States to adopt rules allowing to restrict the obligations on data quality, the rights to information and of access, when necessary to safeguard "(a) national security; (b) defence; (c) public security; (d) the prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions; [...] (f) a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in cases referred to in (c), (d) and (e); (g) the protection of the data subject or of the rights and freedoms of others".

---

99 Articles 10 and 11 of Directive 95/46/EC.
100 Articles 16 and 17 of Directive 95/46/EC.
101 Article 12 Directive 95/46/EC.
102 Case C-614/10, "Commission v. Austria" (2012).
103 Kuner (2010).
104 Article 29 Data Protection Working Party (1998).
105 Article 29 Data Protection Working Party (1998).
106 Joined Cases C-92/09 and C-93/09, "Volker und Markus Schecke GbR and Hartmut Eifert v. Land of Hesse" (2010), paragraph 48.
107 Recital 26 of Directive 95/46/EC.
108 Article 4 Directive 95/46/EC *a contrario*.
109 See article 3 on material scope, recitals 12, 13, 16 and 17 of Directive 95/46/EC.

In line with the original strategy, Regulation 45/2001/EC[110] extends the level of protection afforded by the Directive to the bodies and institutions of the Community by setting up the European Data Protection Supervisor (hereafter EDPS), i.e. the EU data protection ombudsman tasked with supervising, consulting and advising the European Union institutions, bodies and agencies over the application of the Regulation.

Also in line with the original strategy[111], and as urged by the White Paper on Growth[112] and the Bangemann Report,[113] personal electronic data, or data processed in the context of public digital communications networks, were tackled by a *lex specialis*, Directive 97/66/EC, which was repealed by Directive 2002/58/EC.[114]

The e-privacy Directive envisages a similar level of protection as the general Directive, although with some differences. It applies to the processing of data falling within the scope of EU law, in the context of publicly available electronic communications services, in public communications networks only,[115] thus undermining its potential scope of protection (as opposed to including all information society services pullulating on the Internet), further challenged by the repealing Data Retention Directive (see *infra* 2.2.4).

Article 15 extends the scope of application of article 13 of Directive 95/46/EC to the e-privacy Directive, and further specifies it by clarifying that restrictions to the right to privacy must respect the principles of necessity, appropriateness and proportionality, as understood in democratic society, for the safeguarding of "national security, defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorized use of the electronic communications systems."

2.1.3.2 The European Union Charter of Fundamental Rights

Article 6.1 TEU "constitutionalized" the EUCFR: the rights, freedoms and principles set out therein "shall have the same legal values as the treaties." These include article 7 on privacy, and article 8 on data protection, thus recognized as a separate fundamental right. Pursuant to article 51, the EUCFR applies to EU institutions, bodies, offices and agencies and to the Member States when implementing EU law.[116] Articles 7 and 8 represent the latest definition of the right to respect for private and family life and data protection, as laid down by article 52.3, in the EU. According to the Explanations Relating to the Charter of Fundamental Rights[117], which have interpretive value pursuant to articles 52.7 EUCFR and 6.1 TEU, article 7 EUCFR[118] has to be read in line with article 8 ECHR. The only difference between the two descriptions of the right to private life lies in the term 'communications', used instead of 'correspondence', which reflects the technological evolution occurred in the past 60 years. Furthermore, the Explanations clarify that the permissible

---

[110] European Parliament and Council (2001).
[111] European Commission (1990).
[112] European Commission (1993).
[113] Bangemann et al. (1994). The report acknowledged the delay of the EU in developing a profitable e-market, allowed by the World Wide Web boom, vis-à-vis the United States.
[114] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), Official Journal L 201, p. 37-47 (31 July 2002), as modified by the Citizens' Rights Directive in light of the technological changes brought about by the success of the World Wide Web.
[115] Articles 1-3.
[116] Article 51.2. further reads, "The Charter does not extend the field of application of Union law beyond the powers of the Union or establish any new power or task for the Union, or modify powers and tasks as defined in the Treaties." The reference to the "promotion" of rights in the first paragraph suggests a proactive behaviour (Craig and de Bùrca, 2011), which is at odds with the wording of paragraph 2, but which is in line with the non-regression clause contained in article 53, "Nothing in this Charter shall be interpreted as restricting or adversely affecting human rights and fundamental freedoms as recognised, in their respective fields of application, by Union law and international law and by international agreements to which the Union or all the Member States are party, including the European Convention for the Protection of Human Rights and Fundamental Freedoms, and by the Member States' constitutions."
[117] Charter of Fundamental Rights of the European Union. (2007). Official Journal C 303/1, p. 1–22 (14 December 2007).
[118] It lays down "Everyone has the right to respect for his or her private and family life, home and communications."

limitations (as interpreted by the Strasbourg (ECtHR) and Luxembourg (ECJ) case law) shall be the same as those envisaged by article 8.2 ECHR.[119]

As for article 8,[120] the Explanations clarify that this article is inspired by, and derives from the ECHR,[121] Convention 108,[122] article 286 of the Treaty establishing the European Community[123] and Directive 95/46/EC, as well as Regulation (EC) No 45/2001, which "contain conditions and limitations for the exercise of the right to the protection of personal data".[124] Article 8.2 addresses the substantive and procedural principles on processing of personal data.

The substantive principles correspond to the principles listed in articles 6 and 7 of Directive 95/46/EC (and thus the FIPs). Firstly the processing must carried out for legitimate purposes,[125] defined either by the consent of the person or by law (fairness and legitimacy) [126]. Secondly, transparency, i.e. the purposes must be explicit,[127] and the data subject must be adequately informed (transparency).[128] Thirdly, all processing operations, including collection, must be carried out in accordance with the law (legality/lawfulness, which must leave no room for ambiguous interpretations, and be foreseeable, i.e. the consequences of each provision must be known *ex ante*.[129] Fourthly, each processing must relate to a specified, limited purpose (necessity and proportionality, purpose limitation[130]), and the data collected must be adequate, relevant and not excessive.[131] Each new purpose should be connected to a different processing.

The procedural principles correspond to the principles listed in articles 10 to 12 of Directive 95/46/EC: data subjects enjoy the rights to access data concerning him or her, to object to the treatment and to rectify the data whenever incorrect. Article 8.3 represents an acknowledgement of the importance of enforcement for the right to data protection, thus carving in stone the need for oversight by an independent authority.[132]

Articles 7 and 8 must be further read in conjunction with article 52, which can be seen as laying down a "constitutional provision" for permissible limitations. Accordingly, "any limitation on the exercise of the rights and freedoms recognised by this Charter *must be provided for by law* and *respect the essence* of those rights and freedoms. Subject to the principle of *proportionality*, limitations may be made only if they are *necessary* and genuinely *meet objectives of general interest* recognised by the Union or *the need to protect the rights and freedoms of others*."[133]

The Explanations clarify that the wording is based on the case law of the Court of Justice, such as C-292/97,[134] building on *Wachauf*, whereby it was clarified that the exercise of fundamental rights may be restricted insofar as is necessary to pursue objective of general interest of the EU and "do not constitute, with regard to the aim pursued, disproportionate and unreasonable interference

[119] Accession by the EU to the ECHR pursuant to article 6.2 TEU will reinforce such bounds, although, pursuant to article 52.3, EU law can provide more extensive protection.
[120] Article 8 reads, "1. Everyone has the right to the protection of personal data concerning him or her. 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data, which has been collected concerning him or her, and the right to have it rectified. 3. Compliance with these rules shall be subject to control by an independent authority."
[121] Without having a direct counterpart there, although the ECJ has clarified that this provision shall be interpreted in line with the case law of the Strasbourg Court (European Union Network Of Independent Experts On Fundamental Rights, 2006).
[122] In Rotaru v. Romania, the European Court of Human Rights ruled that article 8 ECHR includes the safeguards introduced by Convention 108 (European Union Network Of Independent Experts On Fundamental Rights, 2006).
[123] Now articles 16 and 39 TEU (analysed *infra* 2.1.3.3).
[124] Charter of Fundamental Rights of the European Union. (2007). Official Journal C 303/1, p. 1–22 (14 December 2007), p. 20.
[125] Article 6.a of Directive 95/46/EC.
[126] Id., article 7.
[127] Id., article 6.b.
[128] Id., articles 10-11.
[129] Id., article 6.a.
[130] Id., article 6.b.
[131] Id., article 6.c.
[132] Case C-614/10, "Commission v. Austria" (2012).
[133] Emphases added.
[134] C-292/97 "Karlsson and Others " (2000), paragraph 45.

undermining the very substance of those rights'."[135] General interests include the objectives enshrined in Article 3 TEU, thus including the pursuit of an AFSJ protecting people's rights. Hence, in case of articles 7 and 8, the permissible (i.e. legitimate) limitations, namely those listed in particular in articles 8.2 ECHR, 9 of the Convention 108, 13 of Directive 95/46/EC, and 15 of Directive 2002/58/EC must be proportional to the objective pursued, necessary in a democratic society and meet the objectives of general interest recognized by the Union. Moreover, exceptions must be interpreted restrictively, as any exception,[136] in that they cannot curb the essence of privacy and data protection, whose definition is the objective of section 4.[137]

2.1.3.3 The proposed Regulation: innovation and challenges

The TFEU contains a new legal basis for data protection.[138] Article 16 (former Article 286 TEC) lays down a positive obligation for the legislator to adopt new rules pertaining to the "protection of individuals with regard to the processing of personal data" and the free movement of such data, by EU institutions, bodies, offices and agencies, and by the Member States within the scope of EU law. Such intervention is justified[139] by the impact on privacy and data protection of the combination of advances in technological applications and the changing nature of international data flows, including the interaction between cloud computing[140] and big data bringing about de-anonymisation, growing use of genetic and biometric data, and the increasing reliance by law enforcement agencies (hereafter LEAs) on privately collected data.

Article 16 does not hinge on economic motivations; in keeping with article 8 EUCFR, the protection of personal data is framed as a right. However, article 16 should be read in combination with Declaration n. 20, which clarifies that rules adopted on the basis of article 16 shall provide for specific derogations when affecting directly national security, and Declaration n. 21, encouraging the adoption of specific rules on data processing in the fields of judicial cooperation in criminal matters and police cooperation. Indeed, the Commission has proposed both a Directive regulating data processing in the AFSJ, which is touched upon in section 2.2.5, and a General Regulation.[141] A first analysis of the Commission's 2012 proposal suggests that the system of protection is still based on the 'four building blocks' identified in section 2.1.3.1. For the sake of this paper, we shall focus in particular on 'building blocks' I and IV.

I. Data subjects' (vs. data controllers) informational self-determination based on the notion of personal data and protected by substantive principles. Data subjects endowed with an 'entitlement' to their personal data still lie at the heart of the text. The text broadens the notion of personal data allowing the identification, directly or indirectly, of the natural persons, in the attempt to encompass 17 years of technological divide with Directive 95/46/EC (article 4). The notion of sensitive data (article 9) has also been revised. This category now includes biometric and genetic data, and specifies that children are a new category of particularly sensitive data subjects (article 8). The regulation restyles certain FIPs and proposes new concepts, summarized in articles 5 (principles relating to personal data processing) and 6 (lawfulness of processing). The

---

135 European Parliament (2007), p. 30.

136 C-73/07, "Satakunnan and Satamedia" (2007) paragraph 56; Joined Cases C-92/09 and C-93/09, "Volker und Markus Schecke GbR and Hartmut Eifert v. Land of Hesse" (2010), paragraph 86.

137 With a view to increasing the effectiveness of the EUCFR, the Commission adopted a Fundamental Rights Check-List to be performed for all legislative proposals, which summarizes the order to be performed for permissible limitations (European Commission, 2010b).

138 The article reads, "1. Everyone has the right to the protection of personal data concerning them. 2. The European Parliament and the Council, acting in accordance with the ordinary legislative procedure, shall lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data. Compliance with these rules shall be subject to the control of independent authorities. The rules adopted on the basis of this Article shall be without prejudice to the specific rules laid down in Article 39 of the Treaty on European Union."

139 Article 29 Data Protection Working Party (2009); Buttarelli (2012); Reding (2011).

140 See, for instance, Gayrel (2010); Leenes (2010); Kuner et al. (2012).

141 European Commission (2012b). The specific instrument was chosen with the idea to address the lack of harmonization existing between member states, which affected the equivalent protection of data subjects, and hindered cross-national businesses. While a Regulation could ensure homogeneous protection, the level of safeguards depends on the drafting of an instrument with "teeth".

'openness' FIP, dubbed 'transparency'[142], informs the new rules on information, procedural rights (articles 11 to 15), and remedies (articles 73 to 79).

The Regulation incorporates a concept circulating in academic and technical circles, "Privacy by Design" (hereafter PbD), which relates to the idea that privacy should be the default option, instead of being dependent upon cumbersome ex post procedures requiring considerable operational effort.[143] Article 23 lays down rules on data protection 'by design' and 'by default, paving the way to additional new provisions.'[144] These include new rules on consent (article 7), security and design (articles 30-32), including the concept, taken from the e-privacy Directive, of 'data breaches,' which fall under the responsibility of controllers (chapter IV), whose roles have been redesigned in line with the 'accountability'[145] FIP (responsibility and liability). Controllers shall "ensure and demonstrate for each processing operation the compliance with the provisions of this Regulation". The well-known idea of a life cycle of data, concretized in limits on data retention and in the right to have one's data corrected or deleted, paved the way to two new 'rights': the right to be forgotten and erasure,[146] (article 17), and the right to data portability (article 18). The prohibition of automated decisions is now enshrined in the right to object and the provision on profiling (articles 19 and 20).

IV. Scope of application and restrictions. While the wording of article 2 on the scope of application of the Regulation clarifies some categories (for instance, the Directive will not apply to natural persons' household or personal activities without any gainful interest), its purview is similar to Directive 95/46/EC. As to restrictions, article 21[147] lays down that they should be established by law, and be necessary and proportionate in a democratic society to safeguard interests equivalent to those acknowledged in article 13 of Directive 95/46/EC. Although the provisions allow limitations to be identified by means of Member states law, paragraph 2 clarifies that measures must contain "the objectives to be pursued by the processing and the determination of the controller." Hence, article 21 takes stock of the progressive refinement of safeguards attached to limitations, in particular as provided for by the EUCFR.

[142] It obliges informing data subjects in a clear and straight-forward manner of the data collected, the purpose of the processing and the possible uses made by third parties, the risks involved in such processing, and to whom they should complain in case of a breach of their privacy.

[143] For an early critique of consent, see Rodotà (1973).

[144] More research is needed to highlight the difference between the two concepts, as well as the lack of reference to privacy *tout court*.

[145] Article 29 Data Protection Working Party (2010b); Hustinx (2012b).

[146] Which means withdrawing consent to data processing, whereby "the burden of proof should be on data controllers" (Reding, 2011).

[147] Article 21 reads: "Union or Member State law may restrict by way of a legislative measure the scope of the obligations and rights provided for in points (a) to (e) of Article 5 and Articles 11 to 20 and Article 32, when such a restriction constitutes a necessary and proportionate measure in a democratic society to safeguard: (a) public security; (b) the prevention, investigation, detection and prosecution of criminal offences; (c) other public interests of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, including monetary, budgetary and taxation matters and the protection of market stability and integrity; (d) the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions; (e) a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in cases referred to in (a), (b), (c) and (d); (f)the protection of the data subject or the rights and freedoms of others. 2.In particular, any legislative measure referred to in paragraph 1 shall contain specific provisions at least as to the objectives to be pursued by the processing and the determination of the controller.

2.2 Permissible limitations and security sector-specific legislation adopted in the EU

2.2.1 Council Framework Decision 2008/977/JHA on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters

Directive 95/46/EC does not apply to the processing of personal data concerning public security, defence, state security or the activities of the State in areas of criminal law, nor does it cover the cooperation between police and judicial actors (see *supra* 2.1.3.1).[148] The Council Framework Decision 2008/977/JHA[149] (hereafter 'the Framework Decision') aimed to partially fill the latter gap, by setting data protection limits to the processing of personal data transmitted or made available between member states, [150] for the purpose of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties.[151] The Framework Decision applied basic data protection principles (see *supra* at 2.1.3) to data processing in the area of police and judicial cooperation in criminal matters, while at the same time introducing several exemptions to those same principles.

Firstly, the Framework Decision has a limited scope, as its provisions do not apply to domestic situations (when personal data originate within the Member State which uses them[152]), and to the processing of personal data by Europol, Eurojust, Frontex, the Schengen Information System (SIS), the Customs Information System (CIS) and those allowing the authorities of Member States to access directly certain data systems of other Member States (see *infra* at 2.2.2). The Framework Decision has to be further interpreted 'without prejudice' to essential national security interests and specific intelligence activities in the field of national security.[153]

Secondly, Articles 3.2, 11 and 12.2 taken together provide for a blanket exception to the purpose limitation principle. Personal data may be further processed for purposes additional to those for which they were originally transmitted or made available, such as: "(a) the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties other than those for which they were transmitted or made available; (b) other judicial and administrative proceedings directly related to the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties; (c) the prevention of an immediate and serious threat to public security; or (d) any other purpose only with the prior consent of the transmitting Member State or with the consent of the data subject, given in accordance with national law."[154] According to one scholar, this last provision derogates from the purpose limitation principle so much that it amounts to "purpose deviation."[155] Article 12.2 further states that restrictions on the processing of data may not be applied when sharing the information with other member states or relevant organizations or agencies, unless such restrictions could be applied to similar national data transmissions.

Thirdly, article 13 allows member states to transfer personal data received from another member state to either third states or international bodies if two conditions are fulfilled: the member state from which the data was obtained has given its consent to such a transfer,[156] and the third state or international body concerned ensures an adequate level of protection for the intended data

---

[148] The exclusion of police cooperation was the consequence of the pillar structure under the old regime of the Treaties, "not of the fact that police and judicial data are wholly different" (Hijmans, 2010, p. 227; Reding, 2011).

[149] Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, Official Journal L 350, p. 60 –71 (30 December 2008).

/JHA.

[150] Id., Preamble, recital 7.

[151] Id., Preamble, recital 6.

[152] Id., Preamble, recital 7.

[153] Id., article 1.4.

[154] Id., article 11.

[155] See De Busser (2010), p. 96 concluding that, "the purpose limitation principle is not fully complied with in the Framework Decision on data protection in criminal matters."

[156] Article 13.1.c of Framework Decision.

processing.[157] However, there are several exceptions to these two conditions. Firstly, a transfer without prior consent is permitted if the transfer of such data is essential for the prevention of an "immediate and serious threat" to public security of a member state or a third state or to "essential interests" of a member state, and the prior consent cannot be obtained in good time.[158] The preamble of the Framework Decision specifies that this derogation applies in situations where the nature of a threat "is so immediate as to render it impossible to obtain prior consent in good time". 'Essential interests' of a member state include threats against the critical infrastructure of a member state or serious disruption to a member state's financial system.[159] Secondly, if a third state cannot ensure an adequate level of data protection, personal data can still be transferred in two cases: (a) the national law of the member state transferring the data so provides because of either (i) legitimate specific interests of the data subject, or (ii) legitimate prevailing interests, especially important public interests; or (b) the third state or receiving international body provides safeguards which are deemed adequate by the member state concerned according to its national law.[160] Neither legitimate interests nor public interests are defined in Article 2 of the Decision,[161] which results in a *de facto* impossibility to monitor, let alone control, data transfers of criminal records.[162]

2.2.2 Sector-specific legislation in security-related European data protection

The 2008 Framework Decision provides general rules and principles for police and judicial cooperation in criminal matters. However, this agreement was preceded and supplemented by a number of specific data protection instruments adopted either by AFSJ-related agencies (Europol and Eurojust), or which provided LEAs access to various Schengen databases (SIS, CIS, VIS). These arrangements form the *lex specialis* when they contain specific conditions as to the use of such data by the receiving Member State.[163] When existing laws have a more limited scope, the rules set out in the Framework Decision should be applied.[164]

2.2.2.1 Europol[165] & Eurojust[166]

The Framework Decision applies to the transfer of personal data by Member States to Europol, but it does not affect Europol's or Eurojust's specific data protection mechanisms, including implementing rules such as the Council Acts related to the Europol Rules applicable to Analysis Work Files,[167] Rules governing Europol's relations with partners,[168] Europol Rules on Confidentiality, [169] conditions related to the processing of data for the purpose of determining relevance to Europol's tasks,[170] and Eurojust's rules of procedure on the processing and protection of personal data.[171]

---

157 Id., Article 13.1.d.
158 Id., article 13.2.
159 Id., Preamble, recital 25.
160 Id., article 13.3.
161 Preamble 11 (id.) states that the "legitimate activities of the police, customs, judicial and other competent authorities should not be jeopardised in any way."
162 De Hert (2009).
163 Framework Decision, article 28.
164 Id., Preamble, recital 40.
165 Council Decision 2009/371/JHA of 6 April 2009 establishing the European Police Office (Europol), Official Journal L, p. 121 37–66 (15 May 2009)(hereafter Europol Decision).
166 Council Decision 2002/187/JHA of 28 February 2002 setting up Eurojust with a view to reinforcing the fight against serious crime, Official Journal L 63 p. 1-13 (6 March 2002) (hereafter Europol Decision).
167 Council Decision 2009/936/JHA of 30 November 2009 adopting the implementing rules for Europol analysis work files, Official Journal L 325, p. 14-22, (11 December 2009).
168 Council Decision 2009/934/JHA of 30 November 2009 adopting the implementing rules governing Europol's relations with partners, including the exchange of personal data and classified information, Official Journal L 325, 6-11 (11 December 2009).
169 Council Decision 2009/968/JHA of 30 November 2009 adopting the rules on the confidentiality of Europol information, Official Journal L 332, p. 17-22 (17 December 2009).
170 "Decision of the Management Board of Europol of 4 June 2009 on the conditions related to the processing of data on the basis of Article 10(4) of the Europol Decision."
171 College of Eurojust and European Council (2005).

Europol and Eurojust derogate from general data protection principles in at least two aspects. Both entities allow, under a set of (different) limited circumstances, the processing of sensitive data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, and data concerning health or sex life, and allow for the transfer of personal data to third countries and international organisations in emergency situations.

Article 14.1 of the Europol Decision, for instance, introduces a double limitation to the prohibition of the processing of sensitive personal data. Such processing is permissible when "strictly necessary" for the purposes of the analysis work file concerned and unless such data "supplement other personal data already input in that file".[172] The Decision further specifies that the selection of a particular group of persons solely on the basis of such sensitive data shall be prohibited, since this would be a violation of the purpose of the Analysis Work Files.

Eurojust can process sensitive data only when such data are necessary for the national investigations concerned, as well as for coordination within Eurojust, but such data can never be processed in the index of the Case Management System.[173] Eurojust may also process in "exceptional cases" any type of personal data relating to the circumstances of an offence, "Where they are immediately relevant to and included in ongoing investigations which Eurojust is helping to coordinate."[174]

Furthermore, the Europol Decision allows for the transfer of personal data to public authorities of third countries and international organisations without the consent of the state of origin, or without the existence of a confidentiality agreement, if Europol's director "Considers the transmission of the data to be absolutely necessary to safeguard the essential interests of the Member States concerned within the scope of Europol's objectives or in the interests of preventing imminent danger associated with crime or terrorist offences."[175] Such a decision of the Europol director takes the level of data protection offered by the receiving body into consideration in a much more detailed way than, for instance, the derogation clause in the Framework Decision.[176] A national member of Eurojust can also send personal data to third states and international organisations even when there is no agreement concluded with such an entity, by way of exception and "With the sole aim of taking urgent measures to counter imminent serious danger threatening a person or public security." The national member is responsible for the legality of authorising the communication and has to keep a record of communications of data and of the grounds for such communications. The communication of data shall be authorised only if the recipient gives an undertaking that the data will be used solely for the purpose for which they were requested.[177] Since 2011, Frontex too is allowed to process personal data collected by the Member States during joint operations, pilot projects and rapid interventions. Onward "transmission or other communication" of such personal data processed by the agency to third countries, or other third parties, is prohibited.[178]

---

[172] Analysis work files contain data about persons who are suspected of planning, having committed, taken part in, or witnessed a criminal offence. It also contains data about victims of such an offence, contacts and associates and others persons who can provide information on the criminal offences under consideration. Article 14 ECD.

[173] Eurojust Decision, article 15.4.

[174] Id., article 15.3.

[175] Europol Decision, article 23.8.

[176] The Director has to assess the adequacy of the level of data protection afforded by the receiving entity taking into account all the circumstances relevant to the trans mission of personal data, in particular: (a) the nature of the data; (b) the purpose for which the data is intended; (c) the duration of the intended processing; (d) the general or specific data-protection provisions applying to the entity; (e) whether or not the entity has agreed to specific conditions required by Europol concerning the data. The European Data Protection Supervisor has noted that this provision is properly formulated to ensure the strict application of this particular exemption (European Data Protection Supervisor (EDPS), 2007, p. 29).

[177] Eurojust Decision, article 26.9.

[178] Regulation (EC) 1168/2011 of 25 October 2011 amending Council Regulation No 2007/2004/EC establishing a European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union Official Journal L 304, p. 1-17 (22 November 2011), article 11.a.

2.2.3 Law enforcement access to EU immigration databases

The increasing use by national LEAs and relevant EU agencies, such as Europol and Eurojust, of personal data stored in EU databases that were not exclusively set up for law enforcement purposes, such as Eurodac and the Visa Information system (VIS), represents a very specific type of derogation from the purpose limitation principle. These are not 'security' databases, in the sense that they contain data of individuals that are not directly related to a specific crime. As stated above, exceptions to the purpose limitation principle are possible and may be necessary, as laid down in Article 13 of Directive 95/46/EC and Article 3.2 of Framework Decision 2008/977/JHA, but it is interesting to note that this principle was not seen by the Commission as a "core factor" in the design of at least the VIS and SIS databases, thereby greatly facilitating the possibility of function creep.[179]

VIS was developed in order to improve the EU's common visa policy, by facilitating the exchange of visa data and the verification and identification of visa applicants and holders,[180] in particular with a view to preventing 'visa shopping.' Besides this goal, a separate article made visa-data available for the prevention, detection and investigation of terrorist offences and other serious criminal offences. National authorities may consult VIS data via special access points "in a specific case" and "following a reasoned written or electronic request" if there are "reasonable grounds to consider that consultation of VIS data will substantially contribute to the prevention, detection or investigation of terrorist offences and of other serious criminal offences". Europol may access this data on much looser grounds, namely "within the limits of its mandate and when necessary for the performance of its tasks". [181] However, in "an exceptional case of urgency" such a request can be verified *ex post*. This review includes a check on whether all conditions for access are fulfilled, and whether an exceptional case of urgency indeed existed.[182] VIS data may not be transferred to a third state or organisation, yet "in an exceptional case of urgency, such data may be transferred or made available to a third country or an international organisation exclusively for the purposes of the prevention and detection of terrorist offences, and of other serious criminal offences, and under the conditions set out in that Decision." The prohibition of data transfers is also "without prejudice" to more lenient national law provisions that allow the communication of information on any criminal activity.[183]

The wide purpose of the **SIS** was "to maintain public policy and public security, including national security", in the territories of the Schengen countries.[184] It includes both immigration data (for instance alerts on third country nationals who should be denied entry into the Schengen territory) and criminal data (for instance alerts on persons or vehicles to be placed under surveillance). New purposes were inserted in a regulation in 2004.[185] Although since 2006 it has been decided

---

179 European Commission (2010c), p. 22.

180 Regulation (EC) 767/2008 of 9 July 2008 concerning the Visa Information System (VIS) and the Exchange of Data between Member States on Short-stay Visas, Official Journal L 218, p. 60-81 (13 August 2008), article 2.

181 Id., article 3.1. This article has been subject to debate, with the view put forward that a higher threshold is necessary for allowing access, requiring also the existence of factual indications as the basis for the reasonable grounds mentioned earlier. The Council adopted a separate decision to arrange the modalities of such access. Council Decision 2008/633/JHA of 23 June 2008 concerning access for consultation of the Visa Information System (VIS) by designated authorities of Member States and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offence, Official Journal 218, pp. 129-136 (13 August 2008).

182 Id., article 4; see also article 3.2 VIS Regulation.

183 VIS Regulation, article 3.4. Certain VIS data can also be transferred to a third country "if necessary in individual cases for the purpose of proving the identity of third-country nationals, including for the purpose of return", which is a derogation from the general prohibition on transfer of VIS Data (article 31.2). Such a transfer is subject to a number of conditions listed in article 31.2, and a specific safeguard in article 31.3 states that such transfers "shall not prejudice the rights of refugees and persons requesting international protection, in particular as regards non-refoulement."

184 The Schengen *acquis*, "Convention implementing the Schengen Agreement of 14 June 1985 between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders" 2000, article 96.

185 Council Regulation (EC) 871/2004 of 29 April 2004 concerning the introduction of some new functions for the Schengen Information System, including in the fight against terrorism. Official Journal L 162, p. 29–31 (30 April 2004).

to create a 'second generation' SIS (SIS II), the system is still not operational to date.[186] Most importantly, SIS II provides the legal basis for the inclusion of biometrics (fingerprints and photographs) in SIS. Article 22.c allows to change the nature of the SIS database from a 'hit/no hit' database to a database that may be used to identify a person on the basis of his biometric identifier. In the view of the EDPS the widened access to the SIS, and the addition of new categories of data, have "Caused concerns for years about a shift of purpose of the SIS, from a simple control tool to a reporting and investigation system."[187]

Eurodac was set up in 2003 to facilitate the exchange of fingerprint data of asylum seekers, in order to prevent asylum seekers from filing multiple asylum applications in different member states of the EU. As such, the primary goal of the database is to determine which EU member state is responsible for examining an application for asylum lodged in a EU member state. Since 2005 calls were made to make Eurodac data available to LEAs for the purpose of the prevention, detection and investigation of terrorist offences and other serious criminal offences.[188] As the EDPS noted the first time the Commission proposed such access:

> "The proposals concern the access to personal data of individuals who not only in principle are not suspected of any crime, but are also in need of higher protection because they flee from persecution. These persons represent an especially vulnerable population, and their precarious position has to be taken into account in the assessment of the necessity and proportionality of the proposed action.[189]"

In its amended proposal of 11 October 2010, which was required after the entering into force of the Lisbon Treaty, the Commission withdrew the provision on law enforcement access[190], only to reinsert it in 2012, because it was needed as part of a "balanced deal on the negotiations of the Common European Asylum System package".[191] The EDPS has again questioned the necessity and proportionality of such access, and questioned the introduction of a derogation that would allow LEAs to transmit fingerprint data for immediate comparison in "exceptional cases of urgency", without defining such an exceptional case. In such cases the verifying authority only verifies *ex post* whether all the conditions for a consultation actually existed. [192] The EDPS recommended to add the criterion of the need to prevent an imminent danger associated with serious criminal or terrorist offences, or to add a stricter criterion that resembles preamble 26.[193] The proposed EURODAC Regulation is currently being discussed through trialogues between the Council of the EU, the European Commission and the European Parliament.

2.2.4 The Data Retention Directive

The general trend, whereby LEAs increasingly access data of individuals, who, in principle, are not suspected of committing any crime, informs also the Data Retention Directive.[194] The Directive itself constitutes an exception to the general obligation enshrined in in Article 15(1) of the e-

[186] Regulation (EC) 1987/2006 on the establishment, operation and use of the second generation Schengen Information System (SIS II), Official Journal L 381, p. 4- 23 (28 December 2006); Council Decision 2007/533/JHA on the Establishment, Operation and Use of the Second Generation Schengen Information System (SIS II), Official Journal L 205, p. 63-84 (7 August 2007).

[187] Hustinx (EDPS), (2012a).

[188] See most importantly, European Commission (2009a; 2009b); Meijers Standing Committee of Experts on International Immigration (2009).

[189] European Data Protection Supervisor (EDPS), (2010a).

[190] European Commission (2010a).

[191] European Commission (2012c), at 3.

[192] Id., article 19.3, paragraph 43.

[193] Referring to "a specific and concrete danger associated with a terrorist or other serious criminal offence, or to specific persons in respect of whom there are serious grounds for believing that the persons will commit or have committed terrorist of fences or other serious criminal offences" (European Data Protection Supervisor (EDPS), 2012b).

[194] European Data Protection Supervisor (EDPS), (2005); Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC (Data Retention Directive). Official Journal L 105, p. 54–63 (13 April 2006).

Privacy Directive[195] to erase data when they are no longer needed. [196] Articles 1 and 4 lay down limitations to the obligation to retain data. Accordingly, the data retained shall only be provided to (1) the competent national authorities, (2) in specific cases, (3) for the purpose of the investigation, detection and prosecution of serious crime, as defined by each member state in its national law. For the EDPS, these limitations were not sufficiently precise and recommended to: (1) add a provision to ensure that only the competent authorities can access to the data; (2) clarify that 'specific cases' means that data can only be provided if needed in relation to a specific criminal offence; and (3) limit the purpose to certain serious criminal offences, in order to limit member states' divergences on the concept of 'serious crimes'.[197]

The Data Retention Directive does not provide any further details on the procedures to be followed and the conditions to be fulfilled in order to gain access to retained data, which leaves room for heterogeneous interpretations in the acts transposing the directive into national law. Indeed, an evaluation by the Commission showed that "[M]ost transposing Member States, in accordance with their legislation, allow the access and use of retained data for purposes going beyond those covered by the Directive, including preventing and combating crime generally and the risk of life and limb".[198] The Data Retention Directive will be revised together with the e-Privacy Directive, and, as stated by the Commission, will depend upon the progress of the General Data Protection Regulation. At the time of writing, the Commission has published no specific timetable yet.

2.2.5 The proposed Directive

The Commission's recent proposal for a 'Directive on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data'[199] will replace the Framework Decision 2008/977/JHA. At the same time, however, any provisions enacted prior to the adoption of this Directive will remain unaffected.[200]

The proposal includes a number of new important elements. Firstly, and most importantly, the scope of the Directive is not limited to cross-border data processing anymore. The Directive will apply to all processing activities carried out by 'competent authorities' (as defined in Article 3(14)) for the purposes of the Directive. Secondly, Article 8 of the proposed Directive sets out a general prohibition of processing special categories of personal data, and the exceptions from this general rule, building on Article 8 of Directive 95/46/EC. The article encompasses genetic data, following the decision of the European Court of Human Rights in the *S. and Marper* case. Thirdly, Article 36 spells out the derogations for data transfer based on Article 26 of Directive 95/46/EC, and Article 13 of Framework Decision 2008/977/JHA.

2.3 Impact on existing limitations of international agreements entered into by the EU

The internationalization of domestic security threats leading to the so-called external area of AFSJ,[201] i.e. the overlapping policy sector of the AFSJ and common foreign and security policy

[195] As laid out by Article 15.1 of the e-Privacy Directive: "Member States may adopt legislative measures to restrict the scope of the rights and obligations provided for in Article 5, Article 6, Article 8(1), (2), (3) and (4), and Article 9 (*dealing with the confidentiality of communications, traffic and location data)* of this Directive when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system, as referred to in article 13(1) of Directive 95/46/EC.

[196] Data Retention Directive, article 3.1.

[197] European Data Protection Supervisor (EDPS), (2005), paragraphs 50-56. See also Buttarelli (2011a).

[198] European Commission (2011), p. 8.

[199] European Commission (2012a).

[200] Framework Decision 2008/977/JHA, article 59.

[201] "A concept of internal security cannot exist without an external dimension, since internal security increasingly depends to a large extent on external security. International cooperation […] is essential.

(hereafter CFSP), is playing an ever-growing role in shaping policies concerning the relationship between privacy/data protection and security, due to the value assigned to data by LEAs and the increasing tendency to regulate data exchanges by means of international agreements.

Such overlap may trigger the problem, not resolved by the treaties, of choosing the appropriate legal basis, between articles 16 TFEU and 39 TEU, [202] for data processing activities in the external area of the AFSJ. The problem is not of minor importance, given that the EU and its agencies have entered into a number of important international agreements regulating the exchange of personal data for LEA purposes. Examples include the EU-US Mutual Legal Assistance Agreement, the agreements for the exchange of Passenger Name Records (hereafter PNR) data signed with Canada, Australia and the US, as well as the TFTP agreement with the US[203].

The agreements signed with the US have been the subject of many policy debates, because of the importance of the EU-US relationship, but also due to the increasingly pressing requests of personal data exchanges, informed by the anti-terror policies adopted in the US after 9/11, which have clashed with the EU system of protection of human rights. The frictions that emerged in the last decade originate in an old divergence of views regarding the flow and the role of personal data, which was already evident in the negotiations of the Privacy Guidelines, and which has not been resolved yet. The High Level Contact Group,[204] which was established to foster a common understanding of privacy and data protection informing a common comprehensive data exchange agreement, could not agree on the scope of "law enforcement purposes." Such divergence could affect the very principle of lawfulness as regards the processing and transfer of personal data, in all fields where the US has entered into an agreement with the EU, or one of its agencies.[205]

However, pursuant to article 216 (2) TFEU "Agreements concluded by the Union are binding upon the institutions of the Union and on its Member States." They are part of EU law once entered into force, and thus cannot be at odds with the general principles of EU law, which notably include fundamental rights. If article 39 were chosen as a legal basis, pursuant to article 218 TFEU international agreements would still be subject to the scrutiny of the Court of Justice as to their compatibility with the Treaties. Pursuant to article 21.2(a) TEU, foreign policy and international cooperation action is informed by the safeguarding of EU values (which include human dignity, freedom and the respect for human rights)[206], fundamental interests, security (which is also one of the objectives of the EU, pursuant to article 3 TEU), interdependence and integrity. Action in the area of CFSP shall be guided by the principles that inspired the creation of the EU, which include the universality and indivisibility of human rights and fundamental freedoms, as well as the respect for the principles of the United Nations and international law. Thus, in principle, international agreements could not provide for a lower level of protection of human rights than the one afforded domestically. Nevertheless, an international agreement providing a level of protection equivalent to, or higher than, the one offered within the EU would represent a notable achievement. This is why the Joint Proposal for a Draft of International Standards on the Protection of Privacy with regard to the processing of Personal Data (often referred to as Madrid Resolution),[207] has been warmly received by privacy advocates.

The EU's policies with regard to third countries need to consider security as a key factor and develop mechanisms for coordination between security and other related policies, such as foreign policy" (Council, 2010a, p. 16).

202 Article 39 reads, "In accordance with Article 16 of the Treaty on the Functioning of the European Union and by way of derogation from paragraph 2 thereof, the Council shall adopt a decision laying down the rules relating to the protection of individuals with regard to the processing of personal data by the Member States when carrying out activities which fall within the scope of this Chapter, and the rules relating to the free movement of such data. Compliance with these rules shall be subject to the control of independent authorities" (Cremona, 2012; Hijmans and Scirocco, 2009).

203 For additional information on PNR and the TFTP cases, see Bonfanti et al., (2011).

204 Council. (2009).

205 For a criticism of the international agreements entered into by the EU and its agencies, see De Busser (2012).

206 TEU, article 2.

207 Discussed at the International Conference of Data Protection and Privacy Commissioners, held in Madrid on 5 November 2009.

3. Judicial bodies' interpretation of security limitations to the right to privacy

This section contains the comprehensive comparative review and analysis of recent judgments and legislation in the field of privacy and security, thus fulfilling objective (3), namely analysing European judgments in which the right to privacy was "balanced" with the need to provide security.

3.1 Security and human rights at the ICJ

The International Court of Justice (ICJ), which is one of the principal organs of the United Nations and established through the UN Charter, is primarily an international court for resolving disputes between states. Hence, it would rarely deal with issues that pertain to the fundamental rights of the individual and their relationship to competing rights or interests, such as security.

However, in one if its Advisory Opinions the ICJ did address the theme of this report. In its Advisory Opinion on the *Legal Consequences of a Wall in the Occupied Palestinian Territory*,[208] the Court made a passing reference to the privacy provision of ICCPR article 17 when discussing which human rights of the Palestinians were affected when Israel constructed a security barrier through the Palestinian territory (and not at the Green Line between Israel proper and the occupied Palestinian territory).[209] Thereafter the Court assessed that on the basis of the material available to it, it was not convinced that the specific course chosen by Israel for the wall was necessary to attain its security objectives. As the wall, along the route chosen and its associated security regime, 'gravely infringed' a number of human rights of the Palestinians, its construction by Israel constituted a breach of a number of its international legal obligations[210] and could not be justified with reference to its right of self-defence or a state of necessity.

The ICJ acknowledged that Israel had to face a number of deadly attacks against its civilian population, and that it therefore had not only the right but also the duty to respond in order to protect the life of its citizens. Nevertheless, its measures in doing so had to remain in conformity with international law.[211]

3.2 Human Rights Committee cases

The Human Rights Committee (the monitoring body of the ICCPR, hereafter HRC) has interpreted the permissible limitations to the right to privacy enshrined in article 17 ICCPR in the context of Final Views relating to complaints brought before it, in General Comment n. 16 interpreting article 17 ICCPR, and in concluding observations on government reports on their implementation of the ICCPR.[212]

General Comment n. 16 of the HRC clarifies that article 17 is relative, as suggested by the wording of the article, and is subject to the same limitations and derogations (art. 4 ICCPR) foreseen by the ICCPR for all non-absolute rights (i.e. articles 12, 18, 19, 21 and 22),[213] which are necessary for people to live in society. It shall be recalled that the first clause provides for a negative obligation for the State parties (vertical) and other natural or legal persons (horizontal) to respect individuals' privacy, honour and reputation, unless certain conditions apply to the case. The second clause lays down a positive obligation to ensure that interferences are only allowed, if the criteria mentioned in the first clause are jointly present. Firstly, interferences[214] must be 'lawful' (legal), i.e. provided for by the law of the country, which must be unambiguous, i.e. sufficiently precise to determine when the right can be interfered with, which authorities and organs are

[208] International Court of Justice (2004), p. 136.
[209] Id., paragraph 136.
[210] Id., paragraph 137.
[211] Id., paragraph 141.
[212] Krause and Scheinin (2009).
[213] Nowak (2005).
[214] Attacks against the honour and reputation, which are only given marginal attention in the Comment, and are not analysed in detail here.

allowed to authorize such interferences, the authorities in charge of controlling the former, and how and through which authority or organ individuals can complain. The HRC has reasserted the importance of the principle of lawfulness in the 1995 Concluding Observations on the Russian Federation,[215] referring to the intrusion into private telephone communications, the 1997 Concluding Observations on Jamaica[216] in the context of wiretapping, and the obligation to provide and ensure effective remedies in the 1999 Concluding Observations on Mexico.[217] Secondly, interferences must not be arbitrary, that is reasonable[218] and relevant, i.e. necessary and fulfilling,[219] not capricious,[220] for the circumstances they are addressing, and in line with the provisions, aims and objectives of the ICCPR.[221] Also, interference with the right must be limited to the minimum necessary.[222]

General comment n. 16 has to be read in conjunction with the test for permissible limitations to rights enshrined in the ICCPR[223] elaborated by General Comment n. 27 of 1999 of the Human Rights Committee,[224] whereby restrictions must be lawful, necessary in a democratic society for reaching the legitimate aim and chosen among the least intrusive instruments, "appropriate to achieve their protective function"[225] in proportion to the interest safeguarded, and applied proportionally. Restrictions cannot be applied to the essence of a human right, and must be "consistent with the other rights guaranteed in the Covenant".[226]

Accordingly, the HRC clarified in General Comment n. 16 that prisoners' correspondence should be confidential and integer *de jure* and *de facto*. Prohibitory orders in the context of prisoners' communications have to be narrow [227] Non-arbitrary censorship and control can be applied to prisoners' correspondence,[228] which has to be permitted with families and friends.[229] Home searches should be limited to the gathering of necessary evidence only, and should not amount to harassment. If they do, they are arbitrary, as deemed in the case of Garcìa v. Colombia 687/1996, where Colombian hooded law enforcement agents broke into a house from the roof at 2.00 AM, and verbally abused the inhabiting family members, including children.[230] Likewise, personal body searches must respect the dignity of the searched, and be performed by a person of the same sex,[231] as expressed in the 1995 Concluding Observations on United Kingdom of Great Britain and Northern Ireland 1995.[232] This case dealt with the practice of strip-searching, which was deemed arbitrary in presence of alternative, less intrusive methods. The gathering and use of personal information should be coherent with the principles of purpose limitation, proportionality, transparency and notification, access and rectification (i.e. data protection).[233]

In *Sayadi and Vinck v. Belgium* (1472/2006), the HRC found that the dissemination of the UN Security Council's terrorist list containing full contact details, or personal information about the authors, constituted an attack on their honour and reputation, in view of the negative association that some persons could make between the authors' names and the title of the sanctions list. Moreover, many press articles that cast doubt on the authors' reputation had been published, and

---

215 UN doc. CCPR/C/79/Add. 54 in Blair (2005).
216 UN doc. CCPR/C/79/Add. 83 in id.
217 UN doc. CCPR/C/79/Add. 109 in id.
218 Id.; European Commission of Human Rights (1956).
219 Scheinin (2009a).
220 Nowak (2005).
221 The existence of State laws against the provisions, aims and objectives of the ICCPR, even if not enforced, amount to unlawful interference, as shown by the (non-security related) case of Toonen v. Australia (488/92) (Nowak, 2005; Blair, 2005).
222 Human Rights Committee (1988).
223 Elaborated in the context of article 12 ICCPR, enshrining the right to freedom of movement.
224 Scheinin (2009a).
225 Id., p. 8.
226 Id., p. 8.
227 J. R. T. et al v. Canada 10419/81 in Nowak (2005); Blair (2005).
228 Pinkney v. Canada 27/1977 in Nowak (2005); Blair (2005).
229 Estrella v. Uruguay 74/1980 in Nowak (2005); Blair (2005).
230 Nowak (2005); Blair (2005).
231 Human Rights Committee (1988).
232 UN doc. CCPR/C/79/Add. 55 in Blair (2005).
233 Human Rights Committee (1988).

the authors had needed, on a regular basis, to demand the publication of a right of reply.[234] Hence, a violation of ICCPR article 17 was established. Finally, the Human Rights Committee has stressed that, as a general rule, surveillance "by any technological means" should be prohibited,[235] or allowed only under judicial supervision, as remarked in the 1999 Concluding Observations on Zimbabwe.[236]

3.3 The European Court of Human Rights case law

3.3.1 The court's assessment of the legality of security limitations to the right to private life

The European Court of Human Rights has decided that a security measure that interferes with the right to private life is "in accordance with the law" if the measure has its basis in domestic law and is compatible with the rule of law. It would be contrary to the rule of law, for instance, when a legal discretion granted to the executive is expressed in terms of an unfettered power.[237] Consequently, a domestic law has to include safeguards that constitute "a real curb" on the wide powers afforded to the executive, so as to offer the individual adequate protection against arbitrary interference.[238] The Court has emphasized that such risks of arbitrariness are especially evident where a power of the executive is exercised in secret.[239]

The law must be adequately accessible and foreseeable, that is, formulated with sufficient precision to enable the individual - if need be with appropriate advice - to regulate his conduct. The law must indicate with sufficient clarity the scope of any discretionary power conferred on the competent authorities, and the manner of its exercise.[240] The level of precision required of domestic legislation – which cannot provide for every eventuality – depends to a considerable degree on the content of the instrument in question, the field it is designed to cover, and the number and status of those to whom it is addressed.[241]

In the classic case of *Klass v. Germany*, for instance, the (then) Commission on Human Rights ruled that Germany's law that allowed for secret surveillance measures in the interests of national security and/or the prevention of disorder or crime did contain such safeguards. The law required there to be: (1) factual grounds for suspicion that a person was planning, committing or had committed a serious crime; (2) exhaustion of other less intrusive means; (3) a written and reasoned application by a specified authority which was statutorily empowered to make such an application; (4) a signed authorisation of the measure by a Minister, who (5) had to report monthly to a parliamentary commission on the measures ordered.

The German government stated that it had found the "right balance between the interests of the surveilled individuals and the interests of society in such surveillance."[242] The Commission agreed with this statement,[243] and acknowledged that the German legislator had been able to find the right balance between "The requirements for defending the constitutional democracy and the individual rights." According to the Commission such a "compromise" was inherent in the system of the Convention, since Article 17 made it clear that "Nothing in the Convention may be

[234] Id., p. 23.
[235] Id..
[236] UN doc. CCPR/C/79 Add. 110 in Blair (2005).
[237] "Gillan and Quinton v. UK," (2010) paragraph 77.
[238] Idem, at 79. In this case the Court for instance questioned the fact that (1) there was no requirement to assess the proportionality of authorizing a stop and search measure in a certain area; (2) the ineffectiveness of the temporal and geographical restrictions to the measures provided by Parliament and the review powers of the Independent Reviewer of Terrorism Legislation.
[239] "Malone v. UK" (1984), paragraph 67.
[240] "Gillan and Quinton v. UK" (2010), paragraphs 76-77.
[241] "Gillan and Quinton v. UK" (2010), paragraph 77. In Gillon and Quinton the law did not require a reasonable suspicion of wrongdoing on behalf of a police officer before stopping and searching a person. The lack of such a criterion invites arbitrariness, since there are no criteria against which to judge for instance whether a search had been taken place for racially discriminatory reasons.
[242] "Klass v. Germany " (1977), paragraph 45.
[243] "Id., paragraph 63.

interpreted as implying for any State, group or person any right to engage in any activity or perform any act aimed at the destruction of any of the rights and freedoms set forth therein."[244]

The Court's case-law on the required quality of a law has focussed mostly on wiretapping and other forms of secret surveillance and covert intelligence gathering, which constitute a 'serious' interference with private life and correspondence, and in turn require detailed safeguards to allow their use."[245] The Court indicated that, in order to avoid abuses of power, the following minimum safeguards should be set out in statute law: (1) the nature of the offences which may give rise to the use of the measure; (2) a definition of the categories of people against whom the measures can be used; (3) a limit on the duration of the measure; (4) the procedure to be followed for examining, using and storing the data obtained[246]; (5) the precautions to be taken when communicating the data to other parties; and (6) the circumstances in which recordings may or must be erased or the tapes destroyed.[247] This list has been subsequently quoted as the Court's established position[248] but the Court later added two other criteria, namely (7) that the body issuing authorisations for interception should be independent and (8) that there must be either judicial control or control by an independent body over the issuing body's activity.[249] Interestingly, the Court has ruled that these stringent safeguards must not be necessarily included in laws that allow for GPS-surveillance,[250]since this practice is seen by the Court as less susceptible of interfering with a person's right to respect for private life, because visual or acoustic surveillance "disclose more information on a person's conduct, opinions or feelings."[251] The Court, therefore, only assessed on a more general level whether the law provided adequate protection against arbitrary interference. The German Code of Criminal Procedure did not explicitly allow for GPS surveillance, but the Court agreed with the judicial interpretation of the German domestic courts that it was a "reasonably foreseeable development" that the Code's reference to "other special technical means intended for the purpose of surveillance" covered GPS surveillance.[252] Equally, it found that the domestic law set strict standards for authorising the GPS surveillance as it could only be ordered "Against a person suspected of a criminal offence of considerable gravity or, in very limited circumstances, against a third person suspected of being in contact with the accused, and if other means of detecting the whereabouts of the accused had less prospect of success or were more difficult."[253]

Compared to its wiretapping cases, the Court did not contest the facts that there was no fixed statutory limit on the duration of the GPS monitoring, and that GPS surveillance could be implemented without prior judicial review. The Court found it sufficient, but without elaborating, that the duration of the GPS surveillance in the present case "Was subject to its proportionality in the circumstances and that the domestic courts reviewed the respect of the proportionality principle in this respect."[254] It further acknowledged that the GPS surveillance was not ordered by an investigative judge, but by the prosecutor. However, the Court did not find this problematic, since there was sufficient *ex post facto* judicial review of the surveillance, which offered "sufficient protection against arbitrariness".[255] The Court finished its analysis by crucially concluding that "Sufficient safeguards against abuse require, in particular, that uncoordinated investigation measures taken by different authorities must be prevented and that, therefore, the prosecution, prior to ordering a suspect's surveillance via GPS, had to make sure that it was aware of further surveillance measures already in place"[256] (see *infra* 5.1).

---

244 Id., paragraph 68.
245 "Amann v. Switzerland" (2000), paragraph 56.
246 This includes adding "procedures for preserving the integrity and confidentiality of data", "S and Marper v. UK," 2008, paragraph 99.
247 "Weber and Saravia vs. Germany" (2006), paragraph 95.
248 "Iordachi v. Moldova" (2009), paragraph 39.
249 Id., paragraph 40.
250 Id., paragraph 66.
251 "Uzun v. Germany" (2010), paragraph 52 (emphases added).
252 Id., paragraphs 67-68.
253 Id., paragraph 70.
254 Id., paragraph 69.
255 Id., paragraphs 71-72.
256 Id., paragraph 73.

In the case of S and Marper v. the United Kingdom, the Court further specified the safeguards that should be included in a domestic instrument regulating the use of personal data for police purposes. These safeguards are essentially the same as those outlined in articles 5 to 7 of the Council of Europe's Convention 108: the gathered data should be: (1) relevant: (2) not excessive in relation to the purposes for which they are stored; and (3) preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored.[257] The data must further provide guarantees that (4) the retained data are efficiently protected from misuse and abuse. The Court noted that these safeguards were "especially valid" with regards to the protection of special categories of more sensitive data, "And more particularly of DNA information, which is of great importance to both the person concerned and his or her family." [258] Only when these criteria are fulfilled, the Court is satisfied that domestic law provides an adequate level of protection against arbitrary interference of article 8.

3.3.2 The court's assessment of the proportionality of security measures interfering with the right to private life

For the purposes of this paper it is interesting to note that the Court has not used the doctrine of the 'essence' of a right in cases relating to article 8, which would act as the ultimate limit of a restriction on article 8. This idea is explained by Judge Matscher's dissenting opinion on the scope of Article 5.1, in which he states that the concept of "deprivation of liberty" is not a matter for formal and precise criteria:

> "Quite the contrary - it is a concept of some complexity, having a core which cannot be the subject of argument but which is surrounded by a "grey zone" where it is extremely difficult to draw the line between "deprivation of liberty" within the meaning of Article 5.1 and mere restrictions on liberty that do not come within the ambit of that provision."[259]

Instead, the Court applies a more traditional proportionality test, which is –in Article 8 cases – very similar to its legality test. Even when there is a sound legal basis that passes the Court's legality test, the Court still weighs the interests of a person and the community as a whole in having the right to private life, including the protection of personal data, protected, with the legitimate interest in the detection and prevention of serious crimes.[260] The Court uses the following factors in its proportionality test.

Firstly, the European Court of Human Rights has clarified that an interference with the right to private life will be considered "necessary in a democratic society" for a legitimate aim if it answers a "pressing social need" and, in particular, if it is proportionate to the legitimate aim pursued, and if the reasons adduced by the national authorities to justify it are "relevant and sufficient." [261] It generally takes into account statistical evidence or other examples provided by the Government to assess the reasons for the measure.[262] It also takes into account the nature of the legitimate aim, and the time frame in which a security measure was adopted and subsequently used.[263] The mandatory inclusion of a convicted sex offender in a sex offender database in which personal data were kept for more than 30 years, for instance, was not seen as a disproportionate interference with the right to private life, given that sexual offences were seen as "a particularly reprehensible form of criminal activity" from which children and other vulnerable people had the right to be protected effectively by the State. The database facilitated the identification of potential perpetrators and prevented recidivism.[264]

---

[257] See also Principle 7 of the "Recommendation of the Committee of Ministers regulating the use of personal data in the police sector (Police Recommendation)," (1987).
[258] "S and Marper v. UK" (2008), paragraph 103.
[259] Partly dissenting opinion of Judge Matscher in "Guzzardi v. Italy," (1980), p. 3.
[260] The decision of the Court to see the procedural requirements as a feature of the legality test in Article 8, rather than an element of the proportionality test has been criticized by several authors, including Cameron (2000), paragraph 34.
[261] "S and Marper v. UK" (2008), paragraph 101.
[262] Id., paragraphs 115-117.
[263] "Nada v. Switzerland" (2012), paragraph 186. The Court made a distinction between the threat of terrorism between 1999 and 2002, and the maintaining or reinforcement of targeted sanctions "over the years".
[264] "Bouchacourt v. France" (2009), paragraph 62.

The object and purpose of the ECHR as a human rights treaty further call for its provisions to be interpreted and applied in a manner that renders its guarantees practical and effective. Thus, in order to ensure "respect" for private and family life within the meaning of Article 8, the realities of each case must be taken into account in order to avoid the mechanical application of domestic law to a particular situation. These realities could include the geographical area in which the measures are being imposed, the duration of the measures imposed,[265] the applicant's nationality, age and health,[266] and the risk of stigmatisation.[267]

Thirdly, for a measure to be regarded as proportionate and necessary in a democratic society, the possibility of recourse to an alternative measure that would cause less damage to the fundamental right at issue while fulfilling the same aim must be ruled out.[268]

In any event, the final evaluation as to whether the interference is necessary remains subject to the Court's review of conformity with the requirements of the ECHR. The Court has to determine whether the procedures for supervising the ordering and implementation of the restrictive measures are such as to keep the "interference" to what is "necessary in a democratic society". In addition, the values of a democratic society must be followed as faithfully as possible in the supervisory procedures if the bounds of necessity, within the meaning of Article 8 § 2, are not to be exceeded.[269]

The margin of appreciation tends to be narrower where the right at stake is crucial to the individual's "Effective enjoyment of intimate or key rights. Where a particularly important facet of an individual's existence or identity is at stake, the margin allowed to the State will be restricted."[270] In this context the Court has noted that there is a strong consensus among member states to set limits on the retention and use of DNA data for the detection of crime. This reduces the margin of appreciation of a state to derogate from this standard, especially when the state in question claims to have a "Pioneer role in the development of new technologies."[271] As the Court observed, "The protection afforded by Article 8 of the Convention would be unacceptably weakened if the use of modern scientific techniques in the criminal-justice system were allowed at any cost and without carefully balancing the potential benefits of the extensive use of such techniques against important private-life interests."[272]

3.4 Security-related ECJ case law

3.4.1 Before the entry into force of the Lisbon Treaty: the PNR and Data Retention cases

The jurisprudence of the Court of Justice of the European Union (hereafter ECJ) has developed in line with the expansion of the scope of EU law, which resulted from the evolution of the institutional framework. Before the entry into force of the Lisbon Treaty, the ECJ had limited authority on pronouncing itself on fundamental rights, for which the EU had no general legislative competence, with the exception of interventions that could facilitate the establishment of the internal market.[273] The EUCFR was not binding, and the human rights instruments available were the ECHR, other human rights treaties, and the general principles of EU law. Furthermore, the ECJ could rule on issues strictly pertaining to EU law or the 'first pillar', and thus was not generally

[265] "Nada v. Switzerland" (2012), paragraphs 182 and 195.
[266] Id. In S and Marper the Court attached special importance to the fact that data was gathered of minors "given their special situation and the importance of their development and integration in society" ("S and Marper v. UK" 2008, paragraph 124).
[267] "S and Marper v. UK" (2008), paragraph 122.
[268] See "Glor v. Switzerland" (2009), paragraph 94: "The Court considers that in order for a measure to be considered proportionate and necessary in a democratic society, there must be no other means of achieving the same end that would interfere less seriously with the fundamental right concerned. See also "Malone v. UK" (1984), paragraph 67, saying that the "sufficiency" of a security measure must be balanced against the nature and degree of the interference with the citizen's Convention rights.
[269] "Kvasnica v. Slovakia" (2009), paragraph 80.
[270] "S and Marper v. UK" (2008), paragraphs 101-102.
[271] Id., paragraph 112.
[272] Id.
[273] Advocate General Léger (2005).

competent in the area of police and judicial cooperation disciplined by Title VI of the Treaty on the European Union. The privacy of personal data was regulated by 'first pillar' instruments, namely Directive 95/46/EC and Directive 2002/58/EC, which did not apply to third pillar matters, as clarified by articles 3(2) and 13.1 of the 95/46/EC and 1.3 of the 2002/58. The ECJ confirmed the scope of this limitation in a number of judgements.[274]

The division in pillars has always been problematic. First of all, some large-scale information systems for law enforcement purposes had a legal basis in the first pillar (EURODAC, SIS and VIS).[275] Secondly, data collected in the scope of private sector activities with a purely economic nature, such as the air transport of passengers, and the provision of telecommunication services, progressively acquired relevance for police and judicial bodies, and were at the basis of two notorious cases in court, notably the joint cases C-317/04 and C-318/04, (the so-called 'PNR cases'), and C-301/06 (the Data Retention case). In the three cases, the Court did not provide any interpretation concerning the permissible limitations to the right to privacy with regards to the processing of personal data, as laid down by primary and secondary law.

In the PNR joint cases,[276] the Court considered the formal pleas put forward by the Parliament sufficient ground to annul both Decisions. It declined to express its views on the other pleas, namely the "breach of the fundamental principles of the Directive, breach of fundamental rights and breach of the principle of proportionality" in C-318/04[277] and the "breach of, respectively, the second subparagraph of Article 300(3) EC, Article 8 of the ECHR, the principle of proportionality, the requirement to state reasons and the principle of cooperation in good faith"[278] in C 317/04. In fact, the ECJ addressed the pleas for annulment put forward by the Parliament by means of the so-called essential/ancillary purpose (objective) jurisprudence,[279] in line with the reasoning expressed by Advocate General Léger. In particular, the fact that the data were originally processed in the course and for the purpose of the provision of services within the internal market was deemed merely 'incidental' for the case at hand, since the main objective of the data processing was the protection of "public security for law enforcement purposes"[280] in the context of the fight against terrorism. According to the Advocate General this did not mean that, "Because the PNR data have been collected by private operators for commercial purposes and it is they who arrange for their transfer to a third country, the transfer in question is not covered by that provision. The transfer falls within a framework established by the public authorities that relates to public security."[281] For some authors,[282] the PNR judgments distorted the test *rationae personae* enshrined in article 13 of Directive 95/46/EC, which would *de facto* allow actions by private parties carried out in the framework of policies of the state relating to the AFSJ, to fall outside the scope of the Directive.

---

[274] C-73/07, "Satakunnan and Satamedia," (2007), paragraph 56; "Joined Cases C-92/09 and C-93/09, Volker und Markus Schecke GbR and Hartmut Eifert v. Land of Hesse" (2010), paragraph 86.

[275] Hijmans, and Scirocco (2009).

[276] Joined Cases C-317/04 and C-318/04, European Parliament v. Council and Commission (PNR cases)," (2006). The cases concerned the action for annulment filed by the European Parliament of Council Decision 2004/496/EC and Commission Decision 2004/535 respectively allowing air carriers to transfer Passengers Name Records data to US custom authorities. Passenger name records are data carrying "unverified information provided by passengers and collected by air carriers for enabling reservations" (European Commission, 2010d) p.3, which contain up to 60 fields, including sensitive data (art. 8 Dir. 95/46). In 2001, fulfilling prophecies formulated 30 years before (Rodotà, 1973) the United States starting asking air carriers to transfer to the customs authorities the PNR of all in-bound and outbound flights, as well as of airplane flying across the US air space, pursuant to section 115 of the US Aviation and Transportation security act (ATSA) of 19 November 2001. For a brief account of the matter, see (Privacy International, 2011), available at: https://www.privacyinternational.org/reports/european-union/ii-surveillance-policies#footnote58_2ncyt7r.

[277] C-317/04 and C-318/04, "PNR cases", paragraph 50.

[278] "Id., paragraph 63.

[279] See Case C-426/93, "Germany v Council" (1995), paragraph 33, "The mere fact that an act may affect the establishment or functioning of the internal market is not sufficient to justify using that provision as the basis for the act". See also De Busser (2009).

[280] Advocate General Léger (2005), p. 4752.

[281] C-317/04 and C-318/04, "PNR cases", paragraph 58.

[282] Hijmans and Scirocco (2009).

The same reasoning, based on the essential/ancillary objective, was used in the Data Retention case,[283] although with different results. Ireland[284] challenged the choice of article 95 of the former TEC as the legal basis for Directive 2006/24/EC,[285] and requested the ECJ to annul the Directive. It argued that the facilitation of the pursuit and functioning of the internal market was only an incidental objective of the Directive, while its 'centre of gravity' was rather the investigation, detection and prosecution of crime, including terrorism, akin to the PNR data case. [286] However, the Court supported the opposite reasoning of the defendants,[287] who argued that the Directive's main legal basis was established in the First Pillar.[288] It argued that the main question of this case related to the appropriate division of competence within the Union, and in particular the appropriate choice of legal basis. In the EU, such choice should rest on "objective factors, which are amenable to judicial review, including in particular the aim and content of the measure."[289]

The Court found that article 95 was appropriate both in terms of objectives and content. Hence, even if the main driver for the adoption of Directive 2006/24/EC was the fight to serious crime, including terrorism, which was at that time clearly a third pillar objective, the text of the Directive referred primarily to first pillar activities. Thus, the reasoning applied to the PNR case could not be extended to data retention and, as a consequence, the Court dismissed Ireland's action for annulment. The Commission has taken steps to ensure a correct transposition of the Directive, including by initiating infringement proceedings against a number of member states. Proceedings are still open against the Czech Republic, Germany, Romania and Sweden. On 31 May 2012, the Commission decided to end proceedings against Austria, and to partially withdraw its case against Sweden, as those member states have transposed the Directive. Interestingly, the High Court of Ireland has referred new questions relating to the directive to the European Court of Justice for a preliminary ruling, specifically asking whether the Directive is compatible with articles 7 and 8 EUCFR (see *infra* 3.4.2).[290]

3.4.2 National case studies: data retention

The laws transposing the Data Retention Directive into the member states' jurisdiction have been the objects of cases lodged before several member states' constitutional courts.[291]

Some constitutional courts invalidated the laws transposing the Directive domestically on the basis of their unconstitutionality, as they breach fundamental rights. This is the case of the

[283] "Case C-301/06, "Ireland v Parliament and Council" (2009); Case C-440/05, "Commission v Council" (2007).

[284] Supported by the Slovak Republic.

[285] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC (Data Retention Directive). Official Journal L 105, p. 54–63 (13 April 2006).

[286] Ireland argued that a more appropriate basis for the adoption of Directive 2006/24/EC was to be found in TEU articles 30, 31(1)(c) or 34(2)(b).

[287] Namely Parliament, the Council and the Commission, supported by the European Data Protection Supervisor and the Kingdoms of Spain and the Netherlands.

[288] The common line of reasoning was that, in the aftermath of the terrorist attacks of New York, Madrid and London, many EU countries noticed the potential of the use of traffic data collected by providers of electronic communication services for billing purposes for the detection and prevention of serious crime. As a result, member states began imposing divergent rules on service providers to retain traffic and location data. Since such operation is costly, it was likely to distort competition; for the sake of preventing such distortion, it was necessary to harmonize the rules, thus amending Directive 2002/58, which could only be performed by reference to the same legal basis, article 95. Directive 2006/24/EC uniquely addressed rules pertaining to the proper handling of data to be retained by service provider, and specifically called for the adoption of national rules as far as access and use of the same data by LEAs was concerned.

[289] Case C-440/05, "Commission v Council" (2007), paragraph 60-61.

[290] Case C-293/12, "Reference for a preliminary ruling from High Court of Ireland in the case Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, The Commissioner of the Garda Síochána, Ireland and the Attorney General" (2012).

[291] Article 29 Data Protection Working Party (2004b, 2005, 2006, 2010c); European Data Protection Supervisor (EDPS), (2005).

Romanian Constitutional Court (October 2009),[292] the **Bundesverfassungsgericht** (March 2010),[293] the Supreme Court of **Ireland** (May 2010),[294] and the Supreme Court of **Czech Republic** (March 2011).[295]

The **Romanian Constitutional Court** found that the obligation to retain data for six months infringed the right to privacy. Such obligation would turn the exception into a rule, and eliminate the positive connotation of the right to privacy, which would thus be defined *a contrario* only. As put by the Court, "The regulation of a positive obligation that foresees the continuous limitation of the privacy right and the secrecy of correspondence makes the *essence of the right* disappear by removing the safeguards regarding its execution."[296] Although the Court established that the principle of necessity had not been breached, it found law 298/2008 transposing the Directive into the Romanian jurisdiction entirely unconstitutional, based on the violation of the principles of foreseeability and proportionality.

Referring to the case of *Klass v. Germany*, the Court reminded that the implementation of surveillance measures without adequate and sufficient safeguards can lead to "Destroying democracy on the ground of defending it." Indeed, according to the Court, the language of the law was ambiguous or not sufficiently detailed, thus failing to meet the requirement of foreseeability (accessibility and predictability), as determined by the European Court of Human Rights in *Rotaru vs. Romania*. By means of example, the Court referred to the ambiguous language of article 20 of law 298/2008, which reads, "For the prevention and counteracting the *threats to national security*, the state institutions with attributions in this field *may have* access, under the conditions established by the normative acts that regulate the activity of national security, to the retained data held by the electronic communication services and public networks providers."[297] As a result, the ambiguous ambit of application, coupled with the lack of appropriate and sufficient legal safeguards, determined the disproportionality of law 298/2008. The Romanian Parliament (lower chamber) passed a new Data Retention law last May.[298]

Differently from the Romanian Constitutional Court, the **Bundesverfassungsgericht, or German Federal Constitutional Court**, followed the reasoning of the ECJ in its data retention judgment. It distinguished between data retention and storage – addressed by EU law and taken care of by private parties – and access and use by LEAs – a matter falling within the ambit of national law. While retention may not raise specific constitutional problems, access may be unconstitutional according to how it is implemented. Direct use, especially by the secret services, would raise profiling concerns, and should therefore be strictly limited. Indirect use, i.e. the possibility of obtaining the data from the instances retaining them, would be less risky and therefore need less control.[299] Accordingly, the Bundesverfassungsgericht found the law transposing the Directive only partially unconstitutional, and in particular in breach of article 10.1 of the German Basic Law. Indeed, the transposing law did not satisfy the proportionality test (together with the principle of legality and legitimate aim) set by article 8.2 ECHR, because of a number of criteria.[300] The Court ruled that data retention (for a maximum of six months) could only be allowed in connection with evidence of danger to public security, or suspicion of a serious criminal offence.

---

[292] "Decision no.1258 Regarding the unconstitutionality exception of the provisions of Law no.298/2008 regarding the retention of the data generated or processed by the public electronic communications service providers or public network providers, as well as for the modification of law 506/2004 regarding the personal data processing and protection of private life in the field of electronic communication area," 2009) Available at: http://www.legi-internet.ro/english/jurisprudenta-it-romania/decizii-it/romanian-constitutional-court-decision-regarding-data-retention.html.

[293] "1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08," 2011, available at: https://www.bundesverfassungsgericht.de/entscheidungen/rs20100302_1bvr025608.html.

[294] "Digital Rights Ireland limited vs. the Minister for Communication, Marine, and Natural Reource, the Minister of Justice, Equality and Law Reform, the Commissioner of an Garda Siochana, Ireland and the Attorney General" (2010).

[295] "Judgment 24/10" (2011). Unofficial translation available at https://www.eff.org/node/58471.

[296] Emphasis added. Unofficial translation, available at: http://www.legi-internet.ro/english/jurisprudenta-it-romania/decizii-it/romanian-constitutional-court-decision-regarding-data-retention.html.

[297] Emphases added.

[298] European Digital Rights (EDRI), (2012c).

[299] De Vries et al. (2011).

[300] Id.

The **Czech Constitutional Court**'s judgment stands in between the previous two. On the one hand, the Court challenged the Directive on ground of the necessity principle, expressing doubt "Whether the instrument of universal and preventive traffic and location data retention on almost every electronic communication alone is a necessary and appropriate instrument in terms of the level of privacy infringement affecting enormous number of individuals involved in electronic communication"[301], and with regards to "its original purpose (protection against security threats and prevention of particularly serious criminal activity)."[302]

However, these statements were made in an obiter dictum, while the gist of the decision of annulling the law transposing the Directive was its lack of clarity and proportionality, which breached the right to privacy understood in terms of informational self-determination.[303] The transposing law was found open to abuse, as it did not respect the principle of purpose limitation, it defined the authorities allowed to access the data too broadly, and set unclear procedures regulating the access *tout court*. As stated by the Court, "The mere definition of retention period of "no shorter than 6 month and no longer that 12 months", given the lapse of this period influences the obligation to discard the data, can be deemed ambiguous and with respect to the scope and sensitive nature of retained data entirely insufficient. None of the obligations mentioned does describe rules or methods of meeting such rules in more detail, there is no strict definition of requirements concerning security of retained data, it is not entirely traceable how is the data handled neither on the part of legal entities or natural persons retaining traffic and location data, nor entitled public authorities after requesting the data; the way of discarding such data is not defined either. Further on, there is no definition of liability and respective sanctions in case of breach of such obligations, including missing establishment of the way how affected individuals can seek efficient protection against possible misuse, arbitrariness or non-fulfilment of defined obligations."[304]

The Court further mentioned statistical evidence showing that the data retained was used for petty crimes, in relation to which the Court declared that, "[lower] Courts shall consider primarily the seriousness of crime committed by the act against which criminal proceedings in which the requested data should be used are held." In keeping with the decision of annulment, the Czech Parliament passed amending data retention legislation last August, which will become law as soon as the President of the Republic approves it.[305]

Other Constitutional Courts only invalidated parts of the transposing laws, as is the case of Bulgaria and Cyprus.

The judgment by the constitutional court of **Bulgaria** led to a revision of the transposing laws, namely article 5 allowing LEAs and security personnel to access data retained by providers of Internet and mobile communications without a court order.[306] The Constitutional court of **Cyprus** found the court orders issued under the transposing law unconstitutional, whereas the retention of data was not discussed, due to a provision of the Cypriot constitution that forbids judicial review of legislation "which are necessary for the purpose of complying with obligations as a Member State of the European Union."[307]

In some states, like Hungary and Austria, the cases are still pending before the Constitutional Courts.

---

[301] "Judgment 24/10" (2011), paragraph 55, unofficial translation available at: https://www.eff.org/node/58471 and http://www.slidilove.cz/en/english/english-translation-czech-constitutional-court-decision-data-retention. In paragraph 30, it further stated, "In simple words, under omniscient and omnipresent state and public authority, the freedom of expression, right to privacy and free choice concerning one´s behaviour and actions become basically non-existent and illusory."

[302] "Judgment 24/10" (2011), paragraph 56, unofficial translation available at: https://www.eff.org/node/58471 and http://www.slidilove.cz/en/english/english-translation-czech-constitutional-court-decision-data-retention.

[303] "Judgment 24/10" (2011).

[304] Id., paragraph 51.

[305] Library of Congress Global Legal Monitor, available at: http://www.loc.gov/lawweb/servlet/lloc_news?disp3_l205403313_text. See also European Digital Rights (EDRI), (2012).

[306] European Digital Rights (EDRI), (2008).

[307] Markou (2012), p. 472.

In **Hungary**, the complaint filed by the Hungarian Civil Liberties Union is still pending.[308] It concerns the lack of delimitation of the material scope of application of data retention; in fact, the transposing law does not mention any specific purposes for which the data should be retained.

The **Austrian Verfassungsgerichtshofes** recently filed a request for a preliminary ruling before the Court of Justice of the European Union concerning the interpretation of the EUCFR, as it challenges the compatibility of the Data Retention Directive with the Charter. The Constitutional Court stated in its decision to defer the matter to the Luxembourg Court because "reservations persist concerning the duty to retain data as such, and the consequences that necessarily result therefrom".[309]

A new complaint against the data retention law was recently filed by **Slovak MPs** before the Constitutional Court,[310] including a request for preliminary ruling by the ECJ, if necessary.

In its evaluation report the Commission announced that it would take into account the outcomes of national judgments in its proposal revising the Directive.[311]

3.4.3 The Kadi judgments and the entry into force of the Lisbon Treaty

The (first) Kadi judgement [312] marked a change in the Court's cautious attitude towards the relationship between policies in the AFSJ and the protection of fundamental rights. The joint cases concerned the appeal by Mr. Kadi and Al Barakaat against Council Regulation (EC) No 881/2002 of 27 May 2002, which, pursuant to paragraph 4(b) of Security Council Resolution 1267 (1999), led to the adoption of restrictive measures, namely freezing their funds and other financial resources. According to paragraph 285 of the judgment:

> "It follows from all those considerations that the obligations imposed by an international agreement cannot have the effect of prejudicing the constitutional principles of the EC Treaty, which include the principle that all Community acts must respect fundamental rights, that respect constituting a condition of their lawfulness which it is for the Court to review in the framework of the complete system of legal remedies established by the Treaty."

The judgment is seen as a turning point of the Court's attitude towards fundamental rights,[313] whose importance it fully recognizes, irrespective of the area of policy, thus anticipating the important changes brought about by the Lisbon Treaty.

Firstly, the EUCFR has become legally binding and equivalent to primary law, thus bringing about full recognition of privacy and data protection as fundamental rights (see *supra* 2.1.3.2). As for the right to data protection, article 16 TFEU has direct effects, and the ECJ has explicitly recognized the right for the first time in the Schecke joint cases (cfr. *Oesterreichischer Rundfunk*), although it has so far explicitly avoided to provide any clear definitions of such right. Such innovation detaches the requirement to respect fundamental rights defined in the context of EU law from any internal market objective (despite the oxymoronic provisions of article 51 EUCFR[314]), thus reinforcing the position of human rights in EU law,[315] and provides for an umbrella provision on permissible limitations (article 52).

Moreover, the TFEU 'communitarized' the former title VI TEU or third pillar, which falls within the area of competence of the ECJ (whereas the CFSP is excluded, apart from restrictive measures

---

[308] See at: http://www.statewatch.org/news/2008/may/hungary-data-ret-hclu.pdf.
[309] Verfassungsgerichtshofes Oesterreich, 2012, available at: http://www.vfgh.gv.at/cms/vfgh-site/attachments/2/7/9/CH0003/CMS1355817745350/press_release_data_retention.pdf.
[310] European Digital Rights (EDRI), (2012d).
[311] European Commission (2011).
[312] C-402/05 P and C-415/05, "Kadi I" (2008).
[313] Privacy and data protection issues were only addressed in the amendment to regulation 881/2002. European Data Protection Supervisor (EDPS), (2009a; 2009b).
[314] Accordingly, the EUCFR "does not extend the field of application of Union law beyond the powers of the Union or establish any new power or task for the Union, or modify powers and tasks as defined in the Treaties" while EU institutions and Member States (insofar as they are implementing EU law), shall "respect the rights, observe the principles and promote the application thereof in accordance with their respective powers" (Craig and de Bùrca, 2011).
[315] Even protocol n. 30 on the non-applicability of the Charter in the UK and Poland is interpreted as being merely declarative, in that it does not deny the ECJ's review of the compatibility with the general principles of law in the context of the implementation of EU law (id.).

as provided for by article 275 TFEU), with two caveats. Firstly, in line with article 4 TFEU and the principles of conferral, subsidiarity and proportionality, the AFSJ is an area of shared competence between the EU and the Member States and, pursuant to article 72 TFEU, "national security remains the sole responsibility of each Member State." Secondly, the rules concerning data protection in the field of police and judicial cooperation in criminal matters will be valid for at least an additional five years, unless amended or repealed, pursuant to article 10 of Protocol 36 on Transitional provisions.[316] As a result, the ECJ will have no competence until 2015 on those acts adopted pursuant to the rules contained in the former title VI TEU that have not been amended or repealed.[317]

So far, no cases pertaining to an infringement of privacy and data protection in the AFSJ have been lodged before the Court. However, in a very recent case in the field of AFSJ[318] pertaining to the appraisal of implementing rules (Council Decision 2010/252/EU),[319] the Court wrote, "provisions on conferring powers of public authority on border guards (…) mean than the fundamental rights of the persons concerned may be interfered with to such an extent that the involvement of the European Union legislature is required".[320]

316 Hijmans and Scirocco (2009).
317 Id. There will also be no possibility to lodge a procedure for infringement.
318 C-355/10, "Parliament v Council" (2012). Action for annulment under Article 263 TFEU.
319 According to the Parliament, the implementing rules exceed the limits laid down in article 12(5) of the Regulation EC 562/2006, rule on essential elements by granting border guards far-reaching powers, and thus should be regulated by means of the ordinary legislative procedure and not the comitology procedure.
320 The Court further argued that this requires a weighing exercise, namely a political choice, which goes beyond the scope of additional measures within the meaning of the article 12(5) of the Schengen borders code. Thus the Court agreed that essential elements are laid down by the additional measures. Thus, the Court ruled to annul the contested decision (C-355/10, "Parliament v Council," 2012, paragraph 77).

4. A core/periphery approach? The fundamental norm of the right to privacy and permissible limitations

This section presents an analytical alternative to the security vs. privacy approach, namely the core/periphery approach based on a reinterpretation of Alexy's theory of rights.[321] Accordingly, all human rights or fundamental rights would have an inviolable core sealed in a rule, and a periphery surrounding that core and subject to permissible limitations, such as those foreseen by article 8 ECHR, and articles 7 and 8 of the EUCFR, for privacy and data protection. Such a core/periphery approach to rights, reflected in EUCFR article 52(1), lays the basis for combining compliance with the rights to privacy and data protection and the needs of LEAs when conducting an investigation and, in a more general fashion, privacy and security, as opposed to simple theories of abstract balancing. This section represents the heart of the deliverable, in that it combines and fulfils the objectives set out in the introduction (see *supra* 1).

In the public debate on "privacy vs. security" or more broadly "human rights vs. security", particularly in the counter-terrorism context, the fundamental rights of the individual are often reduced to a mere interest or value. The declared interest or value is then weighed against the competing value of public or national security, resulting in an abstract 'balancing' operation that bypasses the many legal safeguards built into the very idea of fundamental rights and almost invariably results in giving priority to increased security, as it is presumed to correspond to the interests of a wider group of people. In their earlier work within the DETECTER project, two of the authors of the current report addressed this type of 'balancing' as part of their classification of so-called unilateral exceptions through which states were trying to justify intrusions into human rights in the name of combatting terrorism.[322] The right to privacy was identified as one of the first victims of the abstract balancing approach, applied through hasty and far-reaching legislative changes and resulting in the erosion of the right to privacy.[323] But the authors also warned that the blunt use of the balancing metaphor in the public debate was resulting in the extension of 'balancing' to such human rights that do not allow for restrictions, or that are non-derogable even in times of emergency, such as the prohibition against torture or other inhuman treatment.[324]

Some of the General Comments by the Human Rights Committee acting under the International Covenant on Civil and Political Rights (ICCPR) support the position that all or at least many human rights contain an essential, inviolable core. In its General Comment No. 27 of 1999 on freedom of movement (article 12), the Committee for the first time explicated its approach to permissible limitations to a human right that in its ICCPR formulation provides for a proper limitations clause. As a part of its elaboration of an analytical, step-by-step test for the permissibility of restrictions, the Committee used the notion of 'the essence' of a human right and emphasized that any restrictions must never impair that essence.[325] The same position was repeated in relation to all ICCPR rights in a subsequent General Comment No. 31 on general state obligations under the ICCPR (article 2), "In no case may the restrictions be applied or invoked in a manner that would impair the essence of a Covenant right."[326] And in General Comment No. 32 on the right to a fair trial, the Committee identified an essential core also in article 14 of the ICCPR, by outlawing such restrictions to the right to access to court that would "undermine the very essence" of the right.[327] Finally, in its General Comment No. 34 on freedom of expression, the latest one available at the time this report is being finalized, the Committee identified freedom of opinion as the essential core of ICCPR article 19:

---

[321] Scheinin (2009b).
[322] Scheinin and Vermeulen (2011). The article is based on research by the authors within the research project DETECTER (Detection Technologies, Terrorism Ethics, and Human Rights), co-funded by the European Commission under the 7th Framework Programme. See at http://www.detecter.eu/.
[323] Id., p. 49-50.
[324] Id., p. 50.
[325] Human Rights Committee (1999).
[326] Human Rights Committee (2004; 2007). Imposed on States Parties to the Covenant, paragraph 6.
[327] Human Rights Committee (2007), paragraph 18.

"[…], Although freedom of opinion is not listed among those rights that may not be derogated from pursuant to the provisions of article 4 of the Covenant, it is recalled that, "in those provisions of the Covenant that are not listed in article 4, paragraph 2, there are elements that in the Committee's opinion cannot be made subject to lawful derogation under article 4". Freedom of opinion is one such element, since it can never become necessary to derogate from it during a state of emergency"; [328]

and:

"Paragraph 1 of article 19 requires protection of the right to hold opinions without interference. This is a right to which the Covenant permits no exception or restriction."[329]

Building upon the practice of the Human Rights Committee and in particular its General Comment No. 27, one of the current authors proposed in his capacity as United Nations Special Rapporteur, that the inviolability of the essential core of any human right – in that case the right to privacy – is one of the steps in an analytically rigorous test for the permissibility of restrictions. In that context, the elements of a permissible limitations test were condensed as follows:

(a) Any restrictions must be provided by the law (paras. 11–12);

(b) *The essence of a human right is not subject to restrictions* (para. 13);

(c) Restrictions must be necessary in a democratic society (para. 11);

(d) Any discretion exercised when implementing the restrictions must not be unfettered (para. 13);

(e) For a restriction to be permissible, it is not enough that it serves one of the enumerated legitimate aims; it must be necessary for reaching the legitimate aim (para. 14);

(f) Restrictive measures must conform to the principle of proportionality; they must be appropriate to achieve their protective function; they must be the least intrusive instrument amongst those which might achieve the desired result; and they must be proportionate to the interest to be protected (paras. 14–15);

(g) Any restrictions must be consistent with the other rights guaranteed in the Covenant (para. 18).[330]

Positive law formulations of all or many fundamental rights containing an essential or inviolable core can be found in many national constitutions.[331] Also the EUCFR, elevated to the status of being a part of the constituting treaties of the EU through the Treaty of Lisbon (see *supra* 2.1.3.2), corresponds to that approach by proclaiming in its article 52, paragraph 1, as follows:

> "Any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and *respect the essence of those rights and freedoms*. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others."[332]

One way to relate to theories of rights the abovementioned idea of each fundamental right, in this context the right to privacy, containing an inviolable core, is to explain that a broadly formulated fundamental right such as the right to privacy in its entirety and as proclaimed in the UDHR, the ICCPR, the ECHR or the EUCFR constitutes a *principle* in the meaning of Robert Alexy's theory of rights,[333] but at the same time carries a more narrow *rule* as its essential and inviolable core. While principles allow for optimization through a process of weighing and balancing against competing principles, a rule either determines the outcome of a case, or it does not apply at all. The interpretation of a legal norm with the character of a principle is primarily a matter of

---

[328] Committee (2011), paragraph 5.

[329] Id., paragraph 9.

[330] Scheinin (2009a), paragraph 17 (footnotes omitted, emphasis added). The bracketed references to numbered paragraphs relate to General Comment No. 27 by the Human Rights Committee. The same elements for a permissible limitations test were presented by Scheinin and Vermeulen (footnote 321), p. 41.

[331] The best known example is article 19, paragraph 2, of the German Basic Law of 1949 addressing restrictions to fundamental rights: "In no case may the essence of a basic right be affected."

[332] Charter of Fundamental Rights of the European Union. (2007). Official Journal C 303/1, p. 1–22 (14 December 2007). Emphasis added.

[333] See also Postscript in Alexy (1992; 1994; 2008).

assessing its weight in relation to other, competing principles. In contrast, as rules are applied in an all-or-nothing fashion, defining their scope of application is the most important question in their interpretation. If a rule applies, it also determines the outcome of a case. As the validity of principles pertains to the legal order as a whole, they will always apply, but their concrete effect in a case depends on a process of optimization in relation to all other, possibly competing, principles. As a rule determines the outcome of a case within its own scope of application, there can never be genuine conflicts between rules. Rather, rules are applied to determine the proper scope of application of each other, such as in the case of a main rule and an exception.[334]

In short, according to a legal positivist understanding of law, every human right contains a core with the quality of a rule. When a case falls within the properly defined scope of application of that rule, it determines the outcome without any further operation of balancing. Hence, the inviolability of the essential core of any human right is an important step in the assessment of permissible limitations to the broader human right surrounding that core.

As a final word concerning the approach of each human right containing an essential or inviolable core and its application in the case of privacy rights, it needs to be emphasized that the notion of a core is of course just a metaphor. Some human rights are complex umbrella concepts that host a number of quite different substantive elements, or attributes.[335] For instance (see *supra* 2.1.1), the ICCPR article 17 formulation of the right to privacy lists, in addition to privacy itself, also family, home, correspondence, honour and reputation as spheres protected as a human right. It is quite understandable that all or several of such interconnected but nevertheless separately identifiable attributes of a complex human right may contain their own core areas, and a single human rights treaty provision therefore is capable of hosting multiple 'cores'. It may be that the terminology of the EUCFR about 'the essence' of a fundamental right is more understandable than the notion of a 'core'. It is however asserted that this is a mere terminological difference and the underlying idea is the same, namely that each human or fundamental right contains areas, dimensions or attributes that are 'off limits' for purposes of permissible limitations. Speaking of an 'essence' or a 'core' should not be seen as preventing contextual assessment, as the essence or core can be defined through a multitude of factors. For that reason we have preferred the notion of a core, as the word 'essence' would obviously sound essentialist. That said, we are not suggesting that each human right as one and only one 'core' that can be defined in absolute terms and would then remain the same for all situations and all times. Rather, the idea is to say that in respect of a proposed intrusion, there is a need to ask the question whether the intrusion would in one or more respect go too far so that it would penetrate the essence or core of the right.

In this context, the right to privacy could be seen as a right consisting of three areas: one that can never be trespassed upon, an area of protection against illegal limitations to the right, and the zone of permissible limitations to the right. The essential core of the right consists then of what is left over after the permissible limitations test has been carried out. From our observations in section 3.3.1, anonymity of a person's communications and movements may not belong in their entirety to the core of the right to private life – if identifiable– since these aspects of the right to private life are subject to a whole range of limitations that the European Court of Human Rights justifies as necessary elements to prevent or prosecute serious crimes.

More as an illustration than as an effort to be exhaustive, three different approaches for defining the inviolable core of privacy in respect of a proposed intrusion, such as the deployment of a given SOST, are presented here. Clearly, they require further discussion and research before being formulated as proposals that could be subjected to the large-scale participatory assessment of perceptions, to be carried out within the SurPRISE project:

a) **Content**: The category of 'sensitive personal data' might be useful for identifying areas that are so deeply private to an individual that they for that reason would belong to the inviolable core not

[334] For an elaboration and application of Robert Alexy's theory on rules and principles, see Scheinin, 2009a.

[335] The notion of 'attributes' was chosen to refer to the main substantive dimensions of a human rights provision in a project with the UN Office of the High Commissioner for Human Rights to identify indicators for the assessment of compliance with human rights treaties. The methodology for defining the attributes representing each human right was based, inter alia, on the General Comments of the respective treaty body and on an effort to find attributes that as far as possible are at the same time mutually exclusive and taken together comprehensive in relation to the substantive scope of the treaty provision. See, in particular United Nations, (2012), p. 31.

subject to limitations or exceptions. Issues of religion, sexuality and health are intuitively strong candidates for strict protection. A strong version of a content-based definition of the inviolable core of privacy would claim that sensitive personal data should always enjoy absolute protection. European legislation and court cases do not seem to support such a strong version of a content-based definition of the core. LEAs are typically allowed under a strict set of limited circumstances to process sensitive data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, and data concerning health or sex life. A weaker variant would therefore combine the categorization as sensitive personal data with a strong procedural threshold, for example a judicial order.

b) **Relation**: As the right to privacy is largely about choice, in the sense that the individual deserves and expects protection to his or her decision as to with whom to share private information, the inviolable core of privacy can also be sought by identifying certain relationships where the confidence between the parties must always remain protected. Partners in a sexual relationship, or the relationship between lawyer and client, doctor and patient, or priest and parishioner are candidates for such mini-spheres of privacy that may be considered inviolable. An extreme example is of course the very 'right to be left alone', the right of a person not to reveal his or her internal state of mind (including in issues of sexual orientation or religion).[336]

c) **Intrusion**: A third option is to focus on the methods of intrusions into privacy, including through various means of technology. Privacy, or some attributes of privacy, may be considered shielded from intrusions through any covert surveillance, or surveillance through a certain technology, or surveillance without judicial authorization.[337] As a result, the use of some technologies would be subject to a lesser degree of scrutiny than others, while those identified as risking penetration of the inviolable core of privacy would be placed under multiple constraints. For instance, some technologies could be applied only in the investigation of a crime that has already occurred and falls within a narrow list of serious crimes, only in relation to an identified suspect of that crime, and only through a judicial warrant. In parallel, technologies identified as not entailing a risk to the core of privacy could be used by decision of the LEAs themselves and also in the prevention of (any) future crimes. This third approach to locating the core of privacy is ultimately procedural in nature. What is 'off limits' for the police in the prevention of crime as it would breach the core of privacy and thus amount to its violation, may be kept within tolerable limits and under strict control if it is administered by the courts and only applied in the investigation of a specific crime already committed, and only in respect of persons on reasonably grounds suspected as the actual perpetrator of the crime. In the latter context, the procedural guarantees would secure that an interference that *prima facie* appears as entering the core of privacy ultimately leaves the (contextually reinterpreted) core intact, and hence is merely a permissible limitation of privacy, rather than a violation.

Further illustrations of the application of the core/periphery approach to different privacy-intrusive technologies will be provided in the next section.

[336] Here, one can see an analogy with the *forum internum* dimension of freedom of religion as a core element of that human right.

[337] An analogy with freedom of expression can be identified here. Even though civil and even criminal liability for what someone has already published can be seen as a permissible content-based limitation of freedom of expression, advance administrative censorship (confiscation of a newspaper or book before its dissemination) would violate the core of freedom of expression.

5. Assessing new technologies

In this section, we build upon the state of the art of four technologies, as elaborated in the SuRPRISE Report on Surveillance Technology and Privacy Enhancing Design" (D3.1, hereafter 'the Report'), namely (GPS-based) location trackers, smart CCTV, network filtering and surveillance by means of deep-packet inspection (by Internet Service Providers) and surveillance of personal devices by means of Trojan Horses, in order to assess the (legal) acceptability of their application.

The test to determine the acceptability of the use of these new technologies is the permissible limitations test outlined in section 4, whereby all of the following cumulative conditions must be met: (a) any restrictions must be provided by the law; (b) the essence of privacy/data protection is not subject to restrictions; (c) restrictions must be necessary in a democratic society; (d) any discretion exercised when implementing the restrictions must not be unfettered; (e) for a restriction to be permissible, it is not enough that it serves one of the enumerated legitimate aims; it must be necessary for reaching the legitimate aim; (f) restrictive measures must conform to the principle of proportionality, they must be appropriate to achieve their protective function, they must be the least intrusive instrument amongst those which might achieve the desired result, and they must be proportionate to the interest to be protected; and (g) any restrictions must be consistent with other human or fundamental rights.

5.1 GPS location trackers

A GPS tracker is a device that uses the Global Positioning System to determine the precise location of a vehicle, person, or other asset to which it is attached with a range accuracy of 7 to 8 metres.[338] Information about the object's location may be stored within the tracker itself, but it can also be sent continually to another device, such as a computer. According to an amicus brief from, amongst others, Roger L. Easton, the "father of the GPS,"[339] "Most high-quality non-military receivers currently provide better than 3 meter horizontal accuracy", and with the use of augmentation systems, "GPS receivers can pinpoint locations to within a few centimetres."[340] GPS receivers nowadays can weigh a mere 10 grams and have the size of a credit card.[341]

GPS trackers therefore allow for the real-time depiction of every place[342] in which the GPS receiver – and therefore the vehicle or person to which that receiver is attached – is currently located and has been located while the GPS receiver was attached. The analysis of GPS data is in most cases complemented with mapping software that transforms the GPS data into a visual depiction of the movements or routes of a person. Depending on the exact type of tracker used, evidence produced by GPS trackers consists mainly of longitude, latitude, and altitude coordinates showing a person's locations at approximately ten second intervals, and a map of a person's movements created with mapping software.

GPS trackers come in many forms. They can be separate devices which are planted by LEAs onto various objects, but the data generated by smart phones equipped with GPS functionality could equally be used for surveillance purposes, for instance by Trojan horses (see *infra* 5.3.2) injected into such mobile devices or through apps that knowingly or unknowingly collect this data.

GPS tracking is fundamentally different from other tools of visual or acoustic surveillance, because the information that is collected is the result of an automated process that is completely divorced from human observation, and, as such, can be used nonstop for an extended period of time. LEAs can watch how objects are moving in real time of course, but their observations are not a prerequisite for determining where a person has moved, or for producing evidence, since a GPS tracker automatically compiles a highly detailed record of a person's location at regular intervals for a long period of time.

---

[338] US Department of Defense (2008), p. v.
[339] Roger L. Easton is the principal inventor and developer of the Timation Satellite Navigation System, which forms the basis for today's GPS-systems.
[340] Center for Democracy & Technology (2011), p. 10.
[341] Id., p. 11.
[342] In open air, with GPS signal availability.

GPS data can be further used to automatically detect the relationships of a person. A study by the MIT showed that large sets of GPS data not only divulge people's locations, but also are able to identify with over 90% accuracy "a person's workplace colleagues, outside friends and people within a user's circle of friends." [343] As such, the ensuing surveillance is not only more precise and comprehensive than that which can be obtained from human observations, but also it is able to reveal intimate details of a person's life, which would be undetectable otherwise – or undetectable without a significant effort in terms of man-hours and other resources. Prolonged GPS-monitoring is further able to reveal patterns in a user's movements, which can – through a simple search on Google Maps or other crowdsourcing-generated maps– generate knowledge about sensitive personal data of a medical or religious nature.

In the recent Supreme Court case *US v. Jones*, Supreme Court Justice Sotomayor quoted a judgment by the New York Court of Appeals, the highest court in the New York's State court system, which had held that GPS data is able to disclose "indisputably private" trips, such as "trips to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment centre, the strip club, the criminal defence attorney, the by-the-hour motel, the union meeting, the mosque, synagogue or church, the gay bar and on and on."[344] The compilation and storage of GPS data, therefore, potentially uncovers a wide variety of the social relationships (and thereby personal and in many cases deeply private identities) one has, including those confidential relationships that can be seen as an element of the 'core' of the right to privacy. Justice Sotomayor recognized this feature of GPS surveillance, and acknowledged its potential for data mining. She even went as far as labelling GPS surveillance potentially *more* intrusive in comparison with other conventional surveillance techniques, because it evades the ordinary checks that constrain abusive law enforcement practices, namely "limited police resources and community hostility."

The result is that "GPS monitoring – by making available at a relatively low cost such a substantial quantum of intimate information about any person whom the Government, in its unfettered discretion, chooses to track – may alter the relationship between citizen and government in a way that is inimical to democratic society."[345] A core/periphery theory of rights would therefore suggest that only investigations into the most serious offences would justify the combination of GPS data with other datasets. In practice, however, it seems unclear how a judge would be able to prevent law enforcement officials from entering a specific location in a crowd-sourcing tool such as Google Maps in order to get more information about certain facilities that are nearby a suspect's location.

The use of GPS surveillance for law enforcement and national security purposes was the subject of a decision by the European Court of Human Rights for the first time in 2010. In Uzun v. Germany,[346] the German authorities suspected Uzun of participating in offenses committed by a left-wing extremist terrorist organization. After tracking with limited success the movements of Uzun through visual and acoustic surveillance measures, the German Federal Office for Criminal Investigation built a GPS receiver into the car of Uzun's accomplice. The GPS surveillance lasted for roughly three months, and allowed the prosecutors to collect important evidence to indict Uzun.

Until Uzun, the Court's case-law on secret measures of surveillance focused exclusively on visual and acoustic surveillance measures, and it developed a set of safeguards that should be set out in the law in order to avoid abuses of power. In view of the risk of abuse intrinsic to "any system of secret surveillance", the Court has claimed that any such system "Must be based on a law that is particularly precise, especially as the technology available for use is continually becoming more sophisticated."[347] In Uzun, however, the Court distinguished secret GPS surveillance from other forms of surveillance, holding that GPS surveillance is "*by its very nature*" and "*as a rule*", less susceptible of interfering with a person's right to respect for private life, because visual or acoustic surveillance "disclose more information on a person's conduct, opinions or feelings."[348] This is a bold statement, as it could be argued that the principal factor determining the gravity of

[343] Eagle (2006).
[344] "United States v. Jones, Justice Sotomayor concurring opinion" (2012), paragraph 3.
[345] Id., paragraph 4.
[346] "Uzun v. Germany" (2010).
[347] "Kopp v. Switzerland" (1998), p. 72.
[348] "Uzun v. Germany" (2010), paragraph 52 (emphases added).

interference with the right to privacy is not whether a technology detects the locations, movements or expressions of persons, but whether it does so secretly.[349]

The European Court of Human Rights did not take the potential impact of GPS-monitoring on the core of the right to privacy into account when it ruled on the legality and proportionality of the GPS surveillance. The Court rather clarified that its proportionality review would focus on the more general existence of "adequate and effective guarantees against abuse". This assessment depends on all the circumstances of the case, such as the nature, scope and duration of the possible measures, the grounds required for ordering them, the authorities competent to permit, carry out and supervise them, and the kind of remedy provided by the national law."[350]

Such a proportionality test is less strict than the test applied by the Court to other secret surveillance techniques, where the Court requires the inclusion of more safeguards to be set out in statute law in order to avoid abuses. Compared to the cases on wiretapping it reviewed, the Court did not question, for instance, the fact that the German law lacked a fixed statutory limit on the duration of the GPS monitoring, and did not provide for *ex ante* judicial review of the measure. The Court attached more importance to the fact that the GPS surveillance was only carried out for a limited period of time, and in order to investigate very serious crimes. Finally, the Court considered that the existence of "judicial review and the possibility to exclude evidence obtained from an illegal GPS surveillance" constituted a sufficient safeguard against abuse.[351] Weighing all these factors, the Court therefore concluded that the applicant's surveillance via GPS, as carried out in the circumstances of the present case, was proportionate to the legitimate aims pursued and thus "necessary in a democratic society" within the meaning of Article 8(2).[352]

5.2 Smart CCTV surveillance

Smart CCTV cameras add new hardware and software capabilities to CCTV cameras in order to enable "more extensive surveillance of public places."[353] The combination of different "sensor technologies", such as CCTV, sound analysis, facial recognition and motion analysis enables a new dimension of securing and controlling spaces and individuals.[354] These new features would enable smart CCTV to "identify and track" individuals, and "classify and analyse" their behaviour.[355] Ultimately, advances in machine vision research would enable the automated recognition of 'unusual' or 'interesting' predetermined traits, risk factors or situations,[356] which in turn would enable a CCTV-operator to prevent such a situation from happening.

In theory, smart surveillance could be seen as a 'privacy-proof' way of conducting surveillance. If nobody is watching what smart CCTV cameras register, and no recordings are made but of those events that were labelled as 'suspicious' or 'irregular', then smart CCTV cameras could be seen as not invading the right to privacy of innocent passers-by. However, this distinction is less important than one might think. In the end, the European Court of Human Rights does not consider that there is any reason to apply different principles concerning the accessibility and clarity of the rules governing the interception of individual communications, on the one hand, and more general programmes of surveillance, on the other.[357]

The greatest concerns relating to the use of smart surveillance cameras are the underlying definitions of what constitutes an 'abnormal' or 'unusual' behaviour (in contrast to only criminal conduct) that a smart CCTV camera should recognize and monitor, especially when the qualification of behaviour as 'abnormal' varies across different times, locations, cultures, or types of threat. This might lead to human interpretations of existing stereotypes of 'abnormal' and 'unusual' behaviour being programmed into (automated) technical systems. When the definition of a person's behaviour as 'abnormal' depends on such a wide variety of factors, an accurate

[349] See Vermeulen (2013, forthcoming).
[350] "Uzun v. Germany" (2010), paragraph 63.
[351] Id., paragraph 72.
[352] Id., paragraph 80.
[353] For an overview of extra 'camera enhancement tools' see Unabhaengiges Landeszentrum fuer Datenschutz (ULD), 2013, p. 9.
[354] Kremer (2012), p.1.
[355] Unabhaengiges Landeszentrum fuer Datenschutz (ULD) (2013), p. 10.
[356] See also the SMART FP7 project, available at http://www.smartsurveillance.eu/
[357] "Liberty and others v. UK" (2008), at 63.

classification of situations and persons becomes extremely difficult, if not impossible. Moreover, there exists a risk that the use of certain indicators may amount to discrimination, by singling out individuals or social groups for adverse treatment on the basis of incorrect or misleading assumptions.[358] For instance, discrimination might occur if a smart CCTV-camera alerts an operator frequently on the basis of suspicious movements that are in fact linked to practicing a specific faith.

While these forms discrimination might occur in a non-technical environment outside of smart CCTV, they are likely to be further amplified by the automated nature of the technology. Neither CCTV camera operators nor even the LEAs typically have access to the underlying software on which assertions of 'abnormality' or 'unusual behaviour' are made. As such the existing predisposition of the software programmers become an automated factor in the decision making process of camera operators and law enforcement agents, without any path to remedy this deficit. Moreover, automated systems are replicating discretionary judgements that would otherwise be made by human beings on the basis of legal and constitutional guarantees. None of the smart CCTV camera systems discussed here has ever been seriously suggested to be able to evaluate 'probable cause' or similar legislative limitations.

A key feature of smart surveillance technologies is that they are used to monitor identifiable persons as they are moving in publicly accessible places. The European Court of Human Rights has earlier indicated that camera surveillance in public places where no visual data is recorded does not, as such, interfere with the 'individuals' private life.[359] An interference with the right to privacy can occur only when materials obtained through such devices are made public in a manner or degree beyond that normally foreseeable.[360]

The German *Bundesverfassungsgericht* followed the same line of thinking when it ruled on the constitutionality of the use of Automatic Number Plate Recognition (ANPR) cameras. The Court ruled that ANPR cameras did not interfere with the "Right to informational self-determination if the data is deleted without a trace, and without the possibility of being restored in the case of no matches on the wanted list, and if this is guaranteed by legal and technical safeguards."[361] In this way the principle of data minimization is actively promoted: the (temporary) storing of personal data should be limited to what is necessary to achieve the purpose for which the data are gathered and further processed.

If smart surveillance measures want to be compliant with the ECHR, it is clear that they must be based on a particularly precise domestic law, which has to give citizens an adequate indication of the conditions and circumstances in which the authorities are empowered to resort to such measures. The Article 29 Data Protection Working Party pointed out that surveillance performed on "grounds of actual public security requirements, or else for the detection, prevention and control of criminal offences"[362] should respect the requirements of Article 8 ECHR. In particular, it stated that the use of such measures has to be proportionate "to the prevention of concrete risks and specific offences – e.g., in premises that are exposed to such risks, or in connection with public events that are likely reasonably to result in such offences."[363] In order to avoid abuses, an independent authority should have access to the source code of smart surveillance cameras in order to ensure compliance of these technologies with the rule of law.

5.3 Network Filtering, Monitoring and Surveillance

Network filtering, monitoring or surveillance of live traffic are common practices performed on information sent through servers and across networks. They are implemented within communications networks by Internet Service Providers (hereafter ISPs), security agencies, and third party actors for different purposes. As highlighted in SurPRISE Deliverable 3.1, there are several methods of filtering, which allow accomplishing different objectives, but can also be deployed cumulatively, and include: TCP/IP header filtering ('egress filtering'); TCP/IP content

[358] House of Lords (2009a), p. 14; (2009b), p. 14.
[359] "Peck v. UK" (2003); "Perry v. UK" (2003), p. 38.
[360] "Peck v. UK" (2003), p. 62: "to an extent which far exceeded any exposure to a passer-by or to security observation".
[361] "1 BvR 2074/05 and 1 BvR 1254/07" (2008), paragraph 68.
[362] Article 29 Data Protection Working Party (2004), p.13.
[363] Id.

filtering (deep-packet inspection); DNS tampering; HTTP proxy filtering; hybrid TCP/IP and HTTP Proxy filtering; denial of service; domain deregistration; and server take down.[364] LEAs have become increasingly interested in the use of such technologies, in particular for the monitoring of email communications and social networks. In accordance with the technical analysis provided for by Deliverable 3.1, this section focuses on deep-packet inspection (hereafter DPI) and on the targeted surveillance of single devices by means of Trojan horses.

5.3.1 Deep-packet inspection by ISPs

This section focuses on DPI implemented by ISPs, which is a technology capable of extracting user data sent over the networks. It applies to information flows and allows a full analysis of the vast majority of such data – particularly when that data is unencrypted – thanks to its capability of inspecting the payload (i.e. content) of the data packets at each layer of the Open Systems Interconnection (OSI) model. Importantly, DPI's analytical capacity includes the application layer, which contains the most confidential user data, i.e. the content of user communications.

DPI is an "enabling technology"[365], in that its three possible functions can be used for different applications. Firstly, it can perform recognition, that is analysing any parts of the packet(s), including the payload, against specific patterns or features (keywords), and putting the packets in relationship based on such patterns and keywords. This requires the use of data mining techniques, that is, refined algorithms and constantly updated dictionaries of patterns/keywords. Secondly, it can perform notification, i.e. sending alerts in relation to patterns and keywords. Thirdly, DPI engines can implement manipulation, i.e. potentially affect the destiny of packets vis-à-vis their destination, for instance by discriminating against them. Usually DPI engines combining function one and two are called 'passive', while those performing function three are referred to as 'active'; they can also be used online (usually for function one and three) or offline (usually for function two).

There are six generally acknowledged applications of DPI/network filtering. For the purposes of this deliverable, the two most pertinent functions[366] are governmental surveillance (which excludes keeping a list of IP addresses) and censorship/content blocking. Governmental surveillance is often directed at email communications and social networks, and can be performed online or offline. "Whichever approach is chosen, the ISP could reroute the traffic through an encrypted IPsec VPN installed to enable security agencies to have direct access to the [email messages] sent there."[367] As noted in Deliverable 3.1, western governments are increasingly attracted by the possibility of imposing ISPs to embed DPI functions in their systems for surveillance purposes. The UNODC recently published a report on online terrorism, which focuses on the use of the Internet for recruitment and plotting, and which encourages the implementation of Internet surveillance.[368] At the end of November 2012, the International Telecommunications Union adopted a standard for DPI, without considering the observations of civil society.[369]

Such developments need to be closely followed, due to the high level of intrusiveness of DPI, and the limited applicability of PbD solutions.[370] It should suffice to notice that the technology treats all citizens as potential suspects, since it can screen the communications of innocent citizens. DPI falls short of "the naïve, dystopian caricature of a surveillance technology that allows network

[364] Anderson (2008).
[365] Mueller (2011), p. 2. On the subject, see also Bendrath (2010); Del Sesto Jr. (2008); Lee (2009); and in general the dedicated website by the Privacy Commissioner of Canada: http://dpi.priv.gc.ca/.
[366] Three are usually performed by ISPs for their own purposes: firstly, network security (i.e. malware recognition + packet capture & analysis, also performed by Computer Response Emergency Teams), which was the first DPI application that led to the creation of Intrusion Detection and Prevention Systems; secondly, bandwidth management/network visibility (prioritize and deprioritize packets, or modify them); thirdly, profiling for behavioural advertising/monetization. The fourth function, Digital Rights Management (DRM), namely the protection of copyright and intellectual property, which is not a security threat, will be briefly addressed, as the ECJ has pronounced on mandatory DRM by ISPs.
[367] Unabhaengiges Landeszentrum fuer Datenschutz (ULD) (2013), p. 44.
[368] While the possible impact on privacy is acknowledged, the protection of data is portrayed as an obstacle to investigations; at most, data protection rules are relevant for their ability to regulate the use of evidence in court (United Nations Office on Drug and Crime (UNODC), 2012).
[369] Latif (2012).
[370] Unabhaengiges Landeszentrum fuer Datenschutz (ULD) (2013).

operators to effortlessly know and manipulate anything and everything their users are doing," and does not yet constitute the "utopian fantasy" of "a piece of equipment that solves all network problems in a single stroke,"[371] due to the need of a dictionary of patterns and behaviours to work. Yet, the main problem that arises in the context of smart CCTV reappears here. In fact, the determination of what constitutes an 'anomaly' can be made on discriminatory grounds, and on technical parameters that are difficult for LEAs to control and appraise from legal perspective.

Since this paper mainly focuses on the rights to privacy and data protection,[372] the first element to be noted is that DPI could violate the prohibition of processing sensitive data enshrined in article 8 of Directive 95/46/EC, whose respect could only be exempted for "reasons of *substantial*[373] public interest" (article 8.4), and as such could violate one potential element of the core identified in section 4. DPI infringes data protection principles such as openness (the system is secret) and individual participation (users cannot oppose the processing). As such it is always used without the knowledge of the user, which makes it a more intrusive technology to the core of the right to privacy. Since the integrity of the gathered data cannot be verified and unlimited information can be easily accessed and used for a wide variety of purposes, DPI is very hard to square with key data protection principles such as data quality, collection limitation and purpose specification (if the extra data collected leads to further uses than the one initially envisaged). Finally, but crucially, it can breach the prohibition of automated individual decisions enshrined in article 15 of Directive 95/46/EC.

The implementation of DPI in the absence of a legal basis could be 'without right' and qualify as a 'crime' (with the caveats that the impact be significant, i.e. not petty and done 'intentionally') pursuant to the provisions of the Council of Europe's Convention on Cybercrime, which is binding on EU member states, and the related Council Framework Decisions 2005/222/JHA on Attacks against Information Systems[374] (currently under revision). In particular, online, passive or active DPI could amount to illegal interception,[375] laid down by article of 3 of the Cybercrime Convention, which protects the confidentiality of personal data, enshrined in articles 16 of Directive 95/46/EC and 5 of Directive 2002/58/EC. Active DPI could also amount to system interference pursuant to article 5 of the Cybercrime Convention, which forbids the serious hindering of a computer system.[376] As such, the generic use of DPI implemented by ISPs is highly unlikely to pass the very first part of the permissible limitation test.

As for the monitoring of content (i.e. on social networks) and of emails, two *leges generales* come into play. Directive 31/2000 on e-Commerce provides mechanisms of cooperation between LEAs and ISPs, but article 15.1 forbids member states to "Impose a general obligation on providers (…) to monitor the information which they transmit or store, nor a general obligation actively to seek facts or circumstances indicating illegal activity." Directive 2002/58 clearly tries to protect the confidentiality of communications by fostering the adoption of measures preventing unauthorized access thereof,[377] and by prohibiting the monitoring of communications (article 5), although article 15.1 allows member states "*[to]* adopt legislative measures providing for the retention of data for a

---

[371] Mueller (2011), p. 4.

[372] However, compliance with other rights is one of the conditions of the permissible limitations test and can also be used to define the core(s) (e.g.racial discrimination).

[373] Emphasis added.

[374] Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems, Official Journal L 69, p. 67-71 (16 March 2005).

[375] It means listening, monitoring, surveilling or procuring, by technical means (any computer systems or electronic eavesdropping/tapping devices, fixed or wireless, by recording or using software/codes/passwords), computer data not publicly transmitted to, from or within a (single, two, etc.) computer system, including electromagnetic emissions (radiations) from a PC carrying computer data. As clarified by the Explanatory Memorandum, the objective is to protect the right to privacy of any electronic data communications pursuant to article 8 ECHR" (Porcedda, 2012). Article 6 of the Directive repealing Council Framework Decision 2005/222/JHA contains a provision of illegal interception, which is missing from the existing text.

[376] Article 5 protects the legal interest of operators and users to have a system functioning properly. It forbids serious interference with a computer system through inputting, transmitting, damaging, deleting, deteriorating altering or suppressing computer data. This article covers denial of service, which was listed as another form of network filtering (Porcedda, 2012). Decision 2005/222/JHA covers system interference in article 3, whereas the e-privacy Directive addresses it at article 4 (and 13 on spamming).

[377] Recital 3 and 21.

limited period justified on the grounds laid down in this paragraph" (i.e. for the legitimate interest of the EU). "All the measures referred to in this paragraph shall be in accordance with the general principles of Community law, including those referred to in Article 6(1) and (2) of the Treaty on European Union."

As for *leges speciale*s, offline and passive DPI would amount to retention, thus falling within the ambit of the Data Retention Directive, which is prohibited as laid down by recital 13, article 2 (scope) and article 5.2, reading "No data revealing the content of the communication may be retained pursuant to this Directive." Online, active DPI would amount to live interception of content data.

The relevant *lex specialis* here is the Cybercrime Convention, which has been signed by all EU member states, whose ratification has been warmly encouraged by the Council, and which contains rules on the investigation and prosecution of crimes relating to 'content'. Article 21 establishes a legal basis for the (confidential) interception ('collection or recording') by the service provider of content data in real-time, of specified communications transmitted by means of a computer system. Such procedure applies to "a range of serious offences to be determined by domestic law", notably the crimes identified by the Convention in article 2 through to 11 (crimes against the availability, integrity and confidentiality of computer systems; computer-related crimes; child pornography[378]; copyright infringement[379]), and its additional protocol on *Acts of a Racist and Xenophobic Nature*[380] *Committed through Computer Systems (*dissemination of racist and xenophobic material,[381] racist and xenophobic insults,[382] xenophobic motivated threat,[383] and denial, gross minimisation, approval or justification of genocide or crimes against humanity[384]). However, article 14 extends the scope of application of article 21 to "Other criminal offences committed by means of a computer system, and the collection of evidence in electronic form of a criminal offence," such as 'online terrorism'. There is no additional legal basis in the EU for the interception of live content data, which falls within the purview of legal interception regulated by each member state, with the exception of child pornography, and a decision regarding copyright infringement.

5.3.1.1 Child pornography

Article 25 of Directive 2011/92/EU on measures against websites containing or disseminating child pornography, to be transposed into national law by 18 December 2013, allows member states to "1. (…) Take the necessary measures to ensure the prompt **removal of web pages** containing or disseminating child pornography hosted in their territory and to endeavour to obtain the removal of such pages hosted outside of their territory. 2. Member States may take measures

[378] Article 9 outlaws: producing, offering or making available; distributing or transmitting; procuring for oneself or another person; and possessing child pornography, namely (realistic images representing) persons appearing as a minor in sexually explicit conduct through a computer system. Liability does not attach when providers act as 'mere conduit'; medical, scientific and artistic purposes are considered legal (Porcedda, 2012).

[379] Article 10 covers offences related to infringements of copyright and related rights States may limit responsibility under this article, if other remedies (civil or administrative measures) are available and the reservations do not impact negatively on relevant international obligations (id.).

[380] They refer to any material, in any format which can be stored, processed and transmitted by means of a computer system, which leads to either pleading in favour of, encouraging, or urging, both hatred (intense dislike or enmity), discrimination and violence (unlawful use of force), against an individual or a group of people, based on race, colour, descent, national or ethnic group, and religion (id.).

[381] Article 3 refers to the active dissemination or posting or compilation of hyperlinks of racist and xenophobic material to the public, through a computer system. Private communications are excluded (id.).

[382] Article 5 outlaws racist and xenophobic insulting publicly, through a computer system, persons or group of persons, for the reason that they belong to a group identified by colour, race, descent, national/ethnic origin or religion; it excludes private communications (id.).

[383] Article 4 consists in menacing the commission of a serious criminal offence (as determined in domestic law) through a computer system, against a person or a group of persons only on the basis of their belonging to a group identified by colour, race, descent, national/ethnic origin or religion (id.).

[384] Article 6 on denial, gross minimisation, approval or justification of genocide or crimes against humanity mirrors article 3. The provision applies also to future crimes against humanity, provided that the party signing the Protocol recognises the court establishing them (id.).

to **block access to web pages** containing or disseminating child pornography towards the Internet users within their territory. These measures must be set by transparent procedures and provide adequate safeguards, in particular to ensure that the restriction is limited to what is necessary and proportionate, and that users are informed of the reason for the restriction. Those safeguards shall also include the possibility of judicial redress."[385]

The Directive leaves it up to the member states to choose the preferred method to block and take down content, which considerably affects the foreseeability and proportionality (and level of harmonization) of the provision. Moreover, monitoring is the prerogative of LEAs acting within a clear legal framework, whereas it does not align with the commercial purpose of ISPs, thus raising issues of lawfulness within the meaning of articles 6.1.b and 7 of Directive 95/46/EC.[386] Actually, the explanatory memorandum to the Cybercrime Convention specifies that the wording of article 9 takes into account the right to privacy and freedom of thought and expression, which are heavily at risk if blanket measures are adopted. Indeed, the adoption of a blanket measure could affect all three elements potentially constituting the core of privacy (and data protection). As the EDPS noted, "more appropriate safeguards are needed to ensure that monitoring and/or blocking will only be done in a strictly targeted way and under judicial control, and that misuse of this mechanism is prevented by adequate security measures."[387]

The issue is particularly worrisome due to the increasing appeal of public-private partnerships (hereafter PPPs), such as the recently-established Global Alliance,[388] which aims at bringing together governments around the world with a view to: enhancing efforts to identify victims, and ensuring that they receive the necessary assistance, support and protection; advancing efforts to investigate and prosecute cases of child sexual abuse online; increasing public awareness of the risks posed by children's activities online; and reducing the availability of child pornography online and the re-victimization of children. (i.e. filtering). According to the EDPS, "Of particular concern is the lack of clarity surrounding the scope and modalities of cooperation between service providers and law enforcement authorities,"[389] with particular regards to the European Cybercrime Centre[390] (hereafter EC3), which "will have child abuse material online as a main focus."[391] [392]

5.3.1.2 Copyright infringement

Although copyright infringement is not a serious threat, the Cybercrime Convention lists it as one of the serious crimes to which the extensive investigative procedures apply. Digital rights holders have been particularly active in driving the adoption of DPI. In a recent case,[393] the ECJ has ruled that ISPs cannot be obliged to install and run DPI capabilities for the sake of preventing the infringement of **intellectual property rights**, not only because of the costs born by the ISPs infringe the freedom of the provider to conduct its business, but also because it allows general monitoring,[394] which is likely to infringe the fundamental rights to data protection (as well as the freedom to receive or impart information and freedom of expression). As put by the Court:

> "The contested filtering system involves monitoring all or most of the information stored by the hosting service provider concerned (…), has no limitation in time, is directed at all future infringements and is intended to protect not only existing works, but also works that have not yet been created at the time when the system is introduced."[395]

---

[385] Directive 2011/92/EU.
[386] European Data Protection Supervisor (EDPS), 2010b.
[387] European Data Protection Supervisor (EDPS) (2010b), p. 3.
[388] See at: http://ec.europa.eu/dgs/home-affairs/what-is-new/news/news/2012/20121130_02_en.htm#/c_.
[389] Paragraph 43 of the "European Strategy for for a Better Internet for Children". See also: http://ec.europa.eu/information_society/activities/sip/index_en.htm.
[390] European Data Protection Supervisor (EDPS) (2012a). THE EDPS notes that data protection has not been taken sufficiently into account, and that the scope of competences of the centre is too vague ('computer crime' as defined in the Europol Decision).
[391] See at: http://europa.eu/rapid/press-release_IP-12-1308_en.htm?locale=en.
[392] One last problem concerns an overlooked issue, namely the rights of the workers employed to sieve the blocked material to judge its criminal nature. It was recently revealed that Facebook uses low-pay labour to spend hours evaluating what could be very harsh material, without any psychological support.
[393] C-360/10, "SABAM v Netlog NV" (2012).
[394] Prohibited by Article 15(1) of Directive 2000/31.
[395] C-360/10, "SABAM v Netlog NV" (2012), paragraph 45.

The injunction requiring installation of the contested filtering system would involve the identification, systematic analysis and processing of information connected with the profiles created on the social network by its users. The information connected with those profiles is protected personal data because, in principle, it allows those users to be identified."[396]

This judgement may have a considerable impact on all cases concerning threats that are not considered 'serious crime'. Legislation disciplining the use of DPI and network filtering should be swiftly discussed, not only because of the surveillance potential of this technology, but also because of its possible impact on security,[397] and the security vs. privacy debate.[398]

5.3.2 Device surveillance by means of Trojan horses

In this section, we focus on surveillance performed on a specific technical device thanks to the use of a Trojan Horse, which is a program, i.e. a string of code, "that creates a backdoor into a computer. This originally amounted to simply creating a hidden remote access facility. Since the arrival of the Internet, access can be obtained from anywhere on the network." [399] The applications of Trojans, which fully qualify as SOSSs and SOSTs, vary in scope and degree, and range from stealing and deleting data (proper computer crimes), to the point of completely taking over the machine of the user,[400] to monitoring legitimate users, a.k.a. governmental surveillance, which is the application of our interest here.

The use of network and computer surveillance by Trojans allows to perform a wide spectrum of activities within different operating systems, including, but not limited to: "monitoring systems (internet telephony interception, chat logging, file transfers); application/screenshots; application filters; VoIP telecommunication surveillance; listing of installed software; country tracking of the infected device; country tracking on mobile devices via GPS and Cell ID; address book/contact list data exfiltration; execution of programs and processes; inducing system crashes ("Blue screen") or re-booting of device; updates of sending station software on device; de-installation; key loggers; access to cameras & microphones; search for and access to stored computer data, and manipulation of data"[401]. Yet, applications are open-ended; a potential future functionality is the use of "inbuilt speech and facial recognition applications to identify individuals using the device."[402] Moreover, the particular capabilities and human rights impact of the Trojan horse engine depend on how it is configured. For instance, if the de-installation function of the engine has not been properly configured, the engine could keep working, even if it is no longer needed, or could be reinstalled by means of the devices' back-up systems.[403]

Surveillance by Trojans may look advantageous as opposed to DPI, in that it is 'targeted' or 'smart', similarly to the case of smart CCTV. Whereas it does not treat all citizens as potential suspects, Trojans can nonetheless be highly intrusive for its monitoring capability. The impact on

---

396 Id., paragraph 49.

397 "Policing the Internet, *as opposed to securing the computers that populate it*, may be a treacherous remedy. (…) The security problems that plague the Internet may beset the computers that will do the policing as much as the computers being policed. If the government expands spying on the Internet without solving the underlying computer security problems, we are courting disaster" (Diffie and Landau, 2008, pp. 3-4).

398 Cyber-security is becoming an increasingly relevant national security issue, but cyber-security is a buzzword as complicated as 'security' itself. As noted in this section, privacy-infringing monitoring capabilities are used to facilitate investigation of either traditional crimes committed online, or for evidentiary purposes. The point is that information security is fully integrated into the functioning of privacy and data protection: by violating the procedural rules on privacy and the protection of personal data, security is put at risk, too. The implementation of permanent monitoring capabilities would hinder the very security of the infrastructure and the data circulating on it, because they would add flows and backdoors, which could be exploited by malefactors, thus leading to a situation where security (which protects privacy) is traded with surveillance (Landau, 2010).

399 Sommer and Brown (2011), p. 23.

400 That machine can then be used "to hide the real identity of a perpetrator. The taken-over machine, referred to as a zombie, then becomes a platform for any number of further exploits." Ibid.

401 Unabhaengiges Landeszentrum fuer Datenschutz (ULD), 2013, p. 38.

402 Ibid.

403 Id.

the rights to privacy and data protection[404] is similar to generic DPI; the difference is that the security safeguards principle (as regards the device of the monitored individual) is by definition violated. As noted in the case of DPI by ISPs, the respect for the principles of purpose limitation in general, use limitation and accountability depend on whether these technologies have been used with or without right, i.e. in a lawful or unlawful way, in accordance with articles 13 and 7 of Directive 95/46/EC, and article 10 on exceptions of Directive 2002/58/EC.

As stated above, the implementation of Trojan horses in the absence of a legal basis (i.e. 'without right') could qualify as a crime. In particular, a Trojan is a virus[405] or malware,[406] which amounts to data interference within the meaning of article 4 of the Cybercrime Convention[407] and article 4 of Decision 2005/222/JHA. A Trojan is the result of, and allows for, illegal access to parts of, or the whole of, a computer system,[408] as defined by article 2 of the Cybercrime Convention[409] and article 2 of Decision 2005/222/JHA. Data interference and illegal access further violate the provisions on data quality (integrity) pursuant to article 6, and of security enshrined in article 17 of Directive 95/46/EC, as well as article 4, and 4.3 of Directive 2002/58/EC. The use of Trojan horses requires the possession of some kind of 'hacker tools'[410], and as such triggers the applicability of article 6 of the Cybercrime Convention, and article 5 of Decision 2005/222/JHA, on the misuse of devices.[411] Finally, Trojan horses can result in the crime addressed by article 7 on computer-related forgery, which lays down an offence akin to tangible documents forgery, since the manipulation of electronic data (public or private document) with evidentiary value (legal effects) may have the same consequences in misleading a third party.[412]

The use of Trojans can be, in the terminology of the Cybercrime Convention, 'with right' if done in accordance with the permissible limitation test. The Cybercrime Convention lays down a legal basis for the access (search) and securing (seize) of stored computer data (article 19) in computer systems or data storage media, and any other relevant systems lawfully accessible from such computer system. Also, member states have the obligation to adopt legal measures (principle of legality) to the effect that the competent authorities will be able to compel the system master or anybody in possessions of the keys for authentication to provide such information, to enable the access and securing of stored computer data.

In order for Trojans to be legally acceptable, the restrictive measures should be in line with the principles of law (lawfulness), and leave no room for ambiguous interpretation, as elucidated by the ECtHR and the ECJ. The essence of privacy and data protection should be protected, and in particular sensitive data and data that is the product of intimate, confidential relationships shall not be processed, or their use kept to the minimum necessary for the investigation. By means of illustration, sensitive data could be processed (under ethical review, i.e. by a panel of independent

---

404 It should be noted that many more rights are affected; however, the focus of this paper is on privacy and data protection.

405 Council of Europe (2001), paragraph 61.

406 The difference between worms (self-spreading) and viruses (requiting user intervention) is blurring, and the term malware is being used instead (House of Lords, 2007).

407 Article 4 grants protection to stored computer data (or programs), akin to corporeal objects, against intentional damage, deterioration, deletion, suppression and alteration (Porcedda, 2012).

408 A computer system, pursuant to article 1 (a) of the Cybercrime Convention, encompasses any device (hardware or software) or group of interconnected devices performing processing of data (exchanged over the network) according to a program (a set of instructions) automatically, i.e. without human intervention (id.).

409 Article 2 criminalises illegal access, by any means, by individuals or organisations, to a part or whole of a computer system (if a system is public, there is no absence of right). This can be simply hacking, cracking or computer trespass, and can result in impediments, alteration, destruction, breach of information confidentiality or other secrecy, thus leading to other forms of criminal action (id.).

410 Council of Europe, 2001, comment on article 6.

411 Article 6 on misuse of devices addresses the offences in articles 2 and 5 at the source, in that it prohibits the production, sale, procurement for use, import, distribution or making available of devices designed or adapted primarily for committing the offences in 2-5 (Porcedda, 2012).

412 The article outlaws "the (unauthorized) input, alteration (modification), deletion (removal) or suppression (concealment) of computer data" so that data is inauthentic (referring as a minimum to the issuer of the data), but with the objective of making it seem authentic for legal purposes (referring to legal transactions and legally relevant documents), independently from the fact that the data is readable and intelligible. States may require the condition of dishonest intent"(id.).

and trustworthy experts) only if a court order provides for it[413]; otherwise, the data should be promptly discarded, and considered inadmissible as evidence.

Also, unauthorized use must be prohibited: Trojans shall only be used in conjunction with an order issued by the judiciary. Restrictions must be necessary in a democratic society, either by genuinely meeting the objectives of general interest recognised by the EU or by protecting the rights and freedoms of others. The performance of surveillance by Trojan horses must be proportional to the objective pursued and subject to scrutiny. Moreover, it should be necessary and the most appropriate instrument for reaching the legitimate aim it is used for. Restrictions to privacy and data protection must be consistent with safeguards provided by the ICCPR, the ECHR and the EUCFR.

In 2008, the German Constitutional Court ruled that limitations should apply to certain tools to access private data or take control of a personal computer. Following the German State Trojan scandal[414], the German Government declared it would entrust the Federal Criminal Police Office to develop a tool for computer surveillance in line with the requirements of the judgment, and accessible to the DPA. However, internal documents show that the government may be far from reaching this objective. In the meantime, pursuant to the Loppsi2 law, the French police can perform surveillance by means of viruses, provided it has the authorization of a judicial authority.[415]

Similarly to what concluded in section 5.3.1.2, legislation disciplining the use of Trojans, and the production and sale of Trojans in general, should be swiftly discussed and implemented, not only due to the surveillance potential of this technology, but also because of its possible impact on security. In fact, the analysis of the German State Trojan carried out by the Chaos Computer Club and the Bavarian DPA revealed two important elements: firstly, surveillance was implemented in violation of the basic cryptographic standards; secondly, a full review of the engine used ('reverse engineering') was not possible, due to the lack of source code.[416]

Both are considered serious breaches of information security, which could lead to wide-scale misuses of the system by malicious users, whether or not implicated in surveillance operations (i.e. tampering with the evidence to be used in court). Transparency and accountability are considered crucial for a full control conducive to the implementation of proper security of information systems, or cyber-security, which is a growing national security concern. Information security is fully integrated into the functioning of privacy and data protection: by violating the procedural rules on privacy and the protection of personal data, the security of information systems is put at risk, too. This begs the question whose security and what security we are trying to address, a question which should be swiftly discussed. The implementation of security measures when handling the data could be a candidate for the core of data protection.

[413] This is particularly urgent, especially since the use of Trojans takes place in the context of PPPs, or is leased to private companies. As a result, LEAs may not have full control on the functioning of Trojans, especially due to possible lack of competence in ICTs, and should thus be assisted by independent competent technical expertise. See, for instance, Deibert (2003).
[414] Unabhaengiges Landeszentrum fuer Datenschutz (ULD) (2013).
[415] European Digital Rights (EDRI) (2012b).
[416] Unabhaengiges Landeszentrum fuer Datenschutz (ULD) (2013).

6. Conclusion: towards operational concepts

This deliverable discussed the legal facets of the impact on privacy and data protection of the use of SOSTs and SOSSs. However, the final purpose of the analysis conducted so far is to inform the citizens' large-scale participatory assessments in work package 5 in a 'bi-directional' manner.

On the one hand, the legal discussion has to be integrated into the information material for citizens participating in the assessments, and should therefore be translated into laypersons' language. On the other hand, the large-scale participatory assessments are expected to validate the criteria developed here. For instance, we expect it to help testing to what extent there is a shared understanding of what specific dimensions of the broadly formulated category of the rights to privacy and data protection should be understood as inviolable, i.e. not subject to permissible limitations. In particular, it should test the suitability of the framework proposed for evaluating the legal acceptability of the deployment of SOSTs and SOSSs in the European Union.

What follows is a first suggestion of 'operationalization' (in terms of information material, quantitative or qualitative analysis) of the legal analysis.

The norms of the fundamental rights to privacy and data protection

We have described how the norms of the fundamental rights to privacy and data protection evolved in the international instruments and legislation (section 2.1). We have proposed two defining elements that may be seen as informing the legal development of the two rights.

On the one hand, privacy "refers to the sphere of a person's life in which he or she can freely express his or her identity, be it by entering into a relationship with others, or alone," and could thus be seen as a right to identity or personality, which justifies its function as a meta-right, serving as the basis for civil and political rights such as freedom of expression, association, and movement, which could not be effectively enjoyed otherwise. The literature tends to identify *at least* four domains of privacy: bodily, informational (data protection), territorial and relational.

On the other hand, privacy puts normative limits to technological advances and related practices, which enhance human possibilities in either sense, and in particular interfere with autonomy and freedom (home, body and correspondence). In particular, the development of Information and Communication Technologies (ICTs) enabled the trans-border flows of personal data ('the international factor'), which sparked the legal reflections on the need to legally protect the 'digital/electronic persona' with a right to data protection.

→ The large-scale participatory assessment should test to what extent citizens perceive privacy and data protection as fundamental rights, and how they conceptualize them. This could be done as part of the qualitative analysis.

The processing of data in the AFSJ, SOSTs and SOSSs, permissible limitations

Trans-border data flows are particularly prominent nowadays. Firstly, data driven transnational businesses are thriving (i.e. ISPs and information society services based on cloud computing and big data). Secondly, the internationalization of security threats has paved the way to a specific area of policy, the external AFSJ. Thirdly, LEAs are increasingly interested in either collecting data produced in the course of purely private or business activities, or using technologies allowing refined data processing, and ultimately surveillance.

→ The large-scale participatory assessment should shed light on the practices relating to the processing (including disclosure) of personal data for the prevention and investigation of crime (information material).

Contextually, it should test the level of trust in different pubic authorities, including LEAs, and their interaction with private authorities (quantitative analysis).

It should help evaluating the extent to which transparency and accountability of said authorities impact on the level of trust (quantitative/qualitative analysis).

The proliferation of SOSTs and SOSSs intruding on the rights to privacy and data protection led to a legislative and judicial refinement of the common understanding of privacy. The HRC, the ECtHR and the ECJ have consistently, and overtly, avoided to provide strict definitions of the rights to privacy and data protection, thus leaving open the possibility to extend its scope of application to new technologies. However, such an approach has hindered to achieve a definition of what constitutes the essence of the rights to privacy and data protection, which weakens the imposition of clear and strict permissible limitations existing in l*eges generales*, and the many *leges speciales* recently adopted to overseeing the use of SOSTs. We have reviewed such permissible limitations (section 2.2), and in particular their interpretation by the three judicial (or quasi-judicial) bodies – the HRC, the ECtHR and the ECJ – in the context of security related case law, in particular where security and privacy were weighed as competing interests, or the problem was avoided altogether (section 3). The three judicial bodies seem to progressively refine the scope of application of limitations and the principles regulating their implementations in response to technological and procedural advances, although the scope of application is not always clear.

→ *The large-scale participatory assessment should test whether citizens frame the use of SOSTs and SOSSs in terms of concrete trade-offs between security and privacy/data protection (quantitative analysis), for instance by phrasing questions about specific intrusions through selected technologies into spheres regarded as deeply personal.*

In parallel it should highlight the awareness of citizens regarding the legal provisions and norms surrounding the use of SOSSs and SOSTs (quantitative analysis).

It should appraise under what conditions citizens accept that specific SOSSs and SOSTs interfere with concrete dimensions of their rights to privacy and data protection (quantitative analysis).

The core/periphery approach

This deliverable has presented the 'core/periphery' approach as an analytical alternative to the abstract 'security vs. privacy' approach in order to assess which limitations to the right to privacy and the protection of personal data are permissible. Such a core/periphery approach to rights is reflected in EUCFR, article 52(1), and could lay the basis for combining compliance with the rights to privacy and data protection and the needs of law enforcement agencies when conducting an investigation and, in a more general fashion, privacy and security, as opposed to simple theories of abstract balancing.

More as an illustration than as an effort to be exhaustive, three different criteria (content, relation and intrusion) were discussed to determine the scope of the core of the right to privacy. We propose that further research within SurPRISE should seek to identify potential candidates for narrowly formulated core areas (or rules) within the broader sphere of the right to privacy. Such identification can take place in relation to specific privacy-intrusive technologies and questions that have arisen in relation to them.

We have proposed to integrate the core/periphery model within a rigorous test for permissible limitations: (a) any restrictions must be provided by the law; (b) the essence of privacy/data protection is not subject to restrictions; (c) restrictions must be necessary in a democratic society; (d) any discretion exercised when implementing the restrictions must not be unfettered; (e) for a restriction to be permissible, it is not enough that it serves one of the enumerated legitimate aims; it must be necessary for reaching the legitimate aim; (f) restrictive measures must conform to the principle of proportionality; they must be appropriate to achieve their protective function; they must be the least intrusive instrument amongst those which might achieve the desired result; and they must be proportionate to the interest to be protected; and (g) any restrictions must be consistent with other human or fundamental rights.

→ *The large-scale participatory assessment should test whether citizens believe in the existence of elements of privacy/data protection that should not be intruded upon in the fight against serious and petty crimes (table discussion/questionnaire). These could include sensitive data, disclosure to a third country, track movements, shed light on the network of personal relationships, and listening to your communications (quantitative/qualitative analysis).*

It should evaluate whether citizens' perception changes if none/all elements of the test for permissible limitations are respected (quantitative/qualitative analysis).

It should evaluate whether the proposed test can be seen as a workable strategy for the acceptable use of SOSSs and SOSTs.

Specific SOSSs and SOSTs

The criteria that could test the 'legal acceptability' of the adoption of SOSSs and SOSTs were used to discuss the privacy implications of the use of four different technologies: GPS-trackers, smart CCTV and deep-packet inspection by ISPs, and surveillance by means of Trojan horses.

→ *The large-scale participatory assessment should shed light on the extent to which citizens are informed about SOSSs and SOSTs currently in use.*

In particular, the use of specific technologies should help to make the discussion more grounded, and appraise the legal issues analysed above.

In doing so, the work done in this deliverable, and work package 3 in general, is going to be integrated with the model developed within work package 2 so as to feed into further work in work package 4 and beyond.

7. Bibliography

7.1 Academic sources

Alexy, Robert. (1994). *Theorie der Grundrechte, 4*. Frankfurt am Main: Auflage, Suhrkamp Verlag.

Alexy, Robert. (1992). *A Theory of Fundamental Rights* (English translation of *Theorie der Grundrechte).* Oxford University Press.

Alexy, Robert. (2008). Constitutional Rights and Legal Systems. In Joakim Nergelius (Ed.), *Constitutionalism: New Challenges: European Law from a Nordic Perspective*. Leiden: Martinus Nijhoff.

Anderson, Ross, and Steven J. Murdoch. (2008). Tools and Technology of Internet Filtering. In John Palfrey Ron Deibert, Rafal Rohozinski, and Jonathan Zittrain, (Ed.), *Access Denied: The Practice and Policy of Global Internet Filtering*. Cambridge: The MIT Press.

Arendt, Hannah. (2011). *La banalità del male*: Feltrinelli.

Bendrath, Ralf, and Milton Mueller. (2010). The End of the Net as we know it? Deep Packet Inspection and Internet Governance. Retrieved from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1653259.

Bennett, Colin and Charles Raab. (2006). *The Governance of Privacy. Policy Instruments in a Global Perspective*. Cambridge: The MIT Press.

Berners Lee, Tim. (2009). No Snooping. Retrieved from: http://dpi.priv.gc.ca/.

Blair, John. (2005). *The International Covenant on Civil and Political Rights and its (First) Optional Protocol. A short Commentary based on Views, General Comments and Concluding Observations by the Human Rights Committee*. Frankfurt: Peter Lang.

Bonfanti, Matteo, Gloria Gonzales-Fuster, and Maria Grazia Porcedda. (2011). European Union. In Privacy International (Ed.), *Global Surveillance Monitor*.

Cameron, Ian. (2000). *National Security And The European Convention On Human Rights*. The Hague/London/Boston: Kluwer Law International.

Craig, Paul and Gráinne de Búrca. (2011). *EU Law: Text, Cases and Materials*. Oxford University Press.

Cremona, Marise. (2012). The Two (or Three) Treaty Solution: The New Treaty Structure of the EU. In Andrea Biondi. Piet Eeckhout and Stephanie Ripley (Ed.), *European Union Law After the Treaty of Lisbon*. Oxford University Press.

De Busser, Els. (2009). *Data Protection in EU and US Criminal Cooperation: A Substantive Law Approach to the EU Internal and Transatlantic Cooperation in Criminal Matters between Judicial and Law Enforcement Authorities.* Antwerpen: Maklu Uitgevers.

De Busser, Els. (2010). Will the EU be serving its citizens an American meal? *Utrecht Law Review, 6*(1), pp. 86-100.

De Busser, Els. (2012). The Adequacy of an EU-US Partnership. In Ronald Leenes Paul de Hert, and Serge Gutwirth, (Ed.), *European Data Protection: in Good Health?* Dordrecht: Springer.

De Hert, Paul, and Vagelis Papakonstantinou. (2009). The data protection framework decision of 27 November 2008 regarding police and judicial cooperation in criminal matters – A modest achievement however not the improvement some have hoped for. *Computer Law and Security Review 25*(5), 403-414.

Deibert, Ronald J. (2003). Black Code: Censorship, Surveillance, and the Militarisation of Cyberspace. *Millenium - Journal of International Studies, 32*(2), 501-530.

Del Sesto Jr., Ronald W., and Jon Frankel. (2008). How Deep Packet Inspection Changed the Privacy Debate. Retrieved from: http://dpi.priv.gc.ca/.

De Vries, Katerina, Rocco Bellanova, Paul De Hert, and Serge Gutwirth,. (2011). The German Constitutional Court Judgment on Data Retention: Proportionality Overrides Unlimited Surveillance (Doesn‘t It ?). In Yves Poullet Serge Gutwirth, Paul De Hert and Ronald Leenes (Ed.), *Privacy and data protection: an Element of Choice.* Dordrecht: Springer.

Diffie, Withfield, and Susan Landau. (2008). Internet Eavesdropping: A Brave New World of Wiretapping. *Scientific American Magazine,* 4, 22 August 2008.

Eagle, Nathan, and Alex Pentland. (2006). Reality Mining: sensing complex social systems. *Pers Ubiquit Comput 10*, 255–268.

Electronic Privacy Information Centre (EPIC), and Privacy International. (2006). *Privacy & Human Rights 2006: An International Survey of Privacy Laws and Developments*. Washington D.C.: Electronic Privacy Information Centre.

Eriksson, Johan, and Giampiero Giacomello. (2012). Content Analysis in the Digital Age: Tools, Functions, and Implications for Security. In Sandro Gaycken & Jörg Krüger (Ed.), *The Secure Information Society: Ethical, Legal and Political Challenges* (pp. 137-148). Dordrecht: Springer.

European Digital Rights (EDRI). (2008). Bulgarian Court annuls a vague article of the data retention law. *EDRi-gram newsletter, n. 6.24*, from http://edri.org/edri-gram/number6.24/bulgarian-administrative-case-data-retention.

European Digital Rights (EDRI). (2012a). Czech Republic: Data retention - almost back in business, *EDRi-gram newsletter, n. 10.15,* from http://www.edri.org/edrigram/number10.15/czech-republic-new-data-retention-law.

European Digital Rights (EDRI). (2012b). Details on German State Trojan programme, EDRi-gram newsletter, n. 10.20, from http://www.edri.org/edrigram/number10.20/details-german--state-spyware-Staatstrojaner.

European Digital Rights (EDRI). (2012c). Romanian Parliament adopts the data retention law. Again. *EDRi-gram newsletter, n. 10.10*, from http://www.edri.org/edrigram/number10.10/romanian-parliament-adopts-data-retention-law-again.

European Digital Rights (EDRI). (2012d). Slovak Constitutional Court receives data retention complaint. EDRi-gram newsletter, n. 10.19, from http://www.edri.org/edrigram/number10.19/slovak-constitutional-court-data-retention.

European Union Network Of Independent Experts On Fundamental Rights. (2006). *Commentary of the Charter of Fundamental Rights of The European Union*.

Finn, Rachel L., David Wright, and Michael Friedewald. (2013). Seven Types of Privacy. In Ronald Leenes S. Gutwirth Gutwirth, Paul de Hert, and Yves Poullet, (Ed.), *European Data Protection: Coming of Age*. Dordrecht: Springer.

Gayrel, Claire, Jacques Gérard, Jean-Philippe Moniy, Yves Poullet and Jean-Marc Van Gyseghem. (2010). Cloud Computing and its Implications on Data Protection. Paper for the Council of Europe's project on Cloud Computing. Namur: Centre de Recherche Informatique et Droit.

Gellman, Robert. (2012). *Fair Information Peactices: A Basic History (Version 1.89)*.

Hijmans, Hielke. (2010). Recent Developments in Data Protection At European Union Level. *ERA Forum, 11*(2), 219 - 231.

Hijmans, Hielke, and Alfonso Scirocco. (2009). Shortcomings in EU Data Protection in the Third and the Second Pillars. Can the Lisbon Treaty be Expected to Help? *Common Market Law Review, 46*, 1485-1525.

IRISS Project Consortium. (2012). Surveillance, fighting crime and violence, Deliverable D1.1.

Krause, Catarina, and Martin Scheinin. (2009). *International Protection of Human Rights: a Textbook*. Turku: Abo Akademi Institute for Human Rights.

Kremer, Jens. (2012). *On the end of Freedom in Public Spaces: Legal Challenges of Wide Area and Multiple Sensor Surveillance Systems (Draft paper)*. Paper presented at the International Association of Constitutional Law Conference, Sydney.

Kuner, Christopher. (2010). Data Protection Law and International Jurisdiction on the Internet. Parts 1 & 2. *International Journal of Law and Information Technology 18(3)*.

Kuner, Christopher, Fred H. Cate, Christopher Millard and Dan Jerker B. Svantesson. (2012). The challenge of 'big data' for data protection. *International Data Privacy Law, 2(2), pp.47-49*.

Landau, Susan. (2010). *Surveillance or Security? The Risk Posed by New Wiretapping Technologies*. Cambridge: the MIT Press.

Latif, Lawrence. (2012). ITU approves deep packet inspection standard behind closed doors, *The Inquirer.net*, 5 December 2012. Retrieved from http://www.theinquirer.net/inquirer/news/2229964/itu-approves-deep-packet-inspection-standard-behind-closed-doors.

Leenes, Ronald. (2010). Who Controls the Cloud? *Revista de Interent, Derecho y Politica, 11*.

Library of Congress Global Legal Monitor. Czech Republic: Newly Amended Data Retention Law. Retrieved from http://www.loc.gov/lawweb/servlet/lloc_news?disp3_l205403313_text

Markou, Christiana. (2012). The Cyprus and other EU court rulings on data retention: the directive as a privacy bomb. *Computer Law and Security Review, 28*, 468-475.

Morsink, Johannes. (1999). *The Universal Declaration of Human Rights: Origins, Drafting and Intent*. Philadelphia: University of Pennsylvania Press.

Mueller, Milton. (2011). DPI technology from the standpoint of internet governance studies: an introduction (v1.1): Syracuse university school of information studies.

Newman, Abraham L. (2008). *Protectors of Privacy. Regulating Personal Data in the Global Economy*. Ithaca: Cornell University Press.

Nowak, Manfred. (2005). Chapter on Article 17 In Manfred Nowak and Felix Ermacora (Ed.), *UN Covenant on Civil and Political Rights, CCPR Commentary,* (2nd edition), pp. 377-405. Kehl: N.P. Engel.

Porcedda, Maria Grazia. (2012). Data Protection and the Prevention of Cybercrime: the EU as an AREA of Security? *EUI Working Paper* (Law 2012/25, pp. 90). Florence: European University Institute.

Privacy International, and Central European University. (2011). Global Surveillance Monitor, European Union.

Rehof, Lars Adam. (1992). The Universal Declaration of Human rights: A commentary. In Gudmundur Alfredsson Asbjorn Eide, Goran Melander, Lars Adam Rehof and Allan Rosas, with the collaboration of Teresa Swinehart, (Ed.). Norway: Scandinavian University Press.

Rehof, Lars Adam. (1995). The Universal Declaration of Human Rights – Common Standard of Achievement. In Asbjorn Eide and Gudmundur Alfredsson (Ed.), pp. 251-264. Norway: Scandinavian University Press.

Rodotà, Stefano. (1973). *Elaboratori Elettronici e Controllo Sociale*. Bologna: Mulino.

Rodotà, Stefano. (2009). Data Protection as a Fundamental Right. In Yves Poullet Serge Gutwirth, Paul De Hert, Sjaak Nouwt and Cécile de Terwangne (Ed.), *In Reinventing Data Protection?* Dordrecht: Springer.

Sartor, Giovanni. (2010). *L'informatica Giuridica e le Tecnologie dell'Informazione. Corso di Informatica Giuridica*. Torino: Giappichelli Editore.

Scheinin, Martin. (2009b). Terrorism and the Pull of 'Balancing' in the Name of Security. In Martin Scheinin (Ed.), *Law and Security, Facing the Dilemmas* (Law 2009/11). Florence: European University Instite.

Scheinin, Martin, and Mathias Vermeulen. (2011). 'Unilateral Exceptions to International Law: Systematic Legal Analysis and Critique of Doctrines to Deny or Reduce the Applicability of Human Rights Norms in the Fight against Terrorism. *Essex Human Rights Review, 8*, 20-56.

Sommer, Peter, and Ian Brown. (2011). *Reducing Systemic Cybersecurity Risks. OECD/IFP Project on Future Global Shocks*.

SurPRISE Project Consortium. (2011). Description of Work (DoW) of the SurPRISE (Surveillance, Privacy and Security) Project: "A large scale participatory assessment of criteria and factors determining acceptability and acceptance of security technologies in Europe": Seventh Framework Programme, European Commission.

SURVEILLE Project Consortium. (2011). Description of Work of the SURVEILLE Project: "Surveillance: ethical issues, legal limitations and efficiency" Seventh Framework Programme, European Union.

Unabhaengiges Landeszentrum fuer Datenschutz (ULD). (2013). *Report on Surveillance Technology and Privacy Enhancing Design, Deliverable 3.1, SurPRISE Project*.

Vermeulen, Mathias. (2013, forthcoming). Secrecy trumps location: A short paper on establishing the gravity of privacy interferences posed by detection technologies. *Novatic*.

Warren, Samuel and Louis Brandeis. (1890). The right to privacy. *Harvard Law Review, 4*(6).

Westin, Alan. (1967). *Privacy and Freedom*: Atheneum Press.

Zencovich, Zeno. (2001). Articolo 8. Diritto al rispetto della vita privata e familiare. In Benedetto Conforti e Guido Raimondi Sergio Bartole (Ed.), *Commentario alla convenzione Europea per la tutela dei diritti dell'uomo e delle libertà fondamentali*. Padova: Cedam.

7.2 Legislation

7.2.1 Council of Europe

Convention for the Protection of Human Rights and Fundamental Freedoms, CETS No. 5, Rome, (4 November 1950).

European Commission of Human Rights. (1956). *Preparatory work on Article 8 of the European Convention on Human Rights*. Strasbourg: Retrieved from http://www.echr.coe.int/library/COLFRTravauxprep.html.

Recommendation of the Committee of Ministers regulating the use of personal data in the police sector (Police Recommendation), R (87) 15 (17 September 1987).

Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, CETS No. 108, Strasbourg (28 January 1981).

Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and trans-border data flows, Strasbourg (8 November 2001).

Convention on on Cybercrime CETS No. 185, Budapest (23 November 2001).

Explanatory Memorandum to the Cybercrime Convention. (2001) Budapest.

7.2.2 European Union

College of Eurojust and European Council. (2005). *Rules of procedure on the processing and protection of personal data*.

Charter of Fundamental Rights of the European Union. (2007). Official Journal C 303/1, p. 1–22 (14 December 2007).

Consolidated versions of the Treaty on European Union (TEU) and the Treaty on the Functioning of the European Union (TFEU), Official Journal C 83/01 (30 March 2010).

Convention implementing the Schengen Agreement of 14 June 1985 between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders, , OJ L 239, p. 19–62 (22 September 2000).

Council Decision 2002/187/JHA of 28 February 2002 setting up Eurojust with a view to reinforcing the fight against serious crime, Official Journal L 63 p. 1-13 (6 March 2002).

Council Regulation (EC) 871/2004 of 29 April 2004 concerning the introduction of some new functions for the Schengen Information System, including in the fight against terrorism. Official Journal L 162, p. 29–31 (30 April 2004).

Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems, Official Journal L 69, p. 67-71 (16 March 2005).

Council Decision 2007/533/JHA on the Establishment, Operation and Use of the Second Generation Schengen Information System (SIS II), Official Journal L 205, p. 63-84 (7 August 2007).

Council Decision 2008/633/JHA of 23 June 2008 concerning access for consultation of the Visa Information System (VIS) by designated authorities of Member States and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offence, Official Journal 218, pp. 129-136 (13 August 2008).

Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, Official Journal L 350, p. 60 –71 (30 December 2008).

Council Decision 2009/371/JHA of 6 April 2009 establishing the European Police Office (Europol), Official Journal L, p. 121 37–66 (15 May 2009).

Council Decision 2009/934/JHA of 30 November 2009 adopting the implementing rules governing Europol's relations with partners, including the exchange of personal data and classified information, Official Journal L 325, 6-11 (11 December 2009).

Council Decision 2009/936/JHA of 30 November 2009 adopting the implementing rules for Europol analysis work files, Official Journal L 325, p. 14-22, (11 December 2009).

Council Decision 2009/968/JHA of 30 November 2009 adopting the rules on the confidentiality of Europol information, Official Journal L 332, p. 17-22 (17 December 2009).

Decision of the Management Board of Europol of 4 June 2009 on the conditions related to the processing of data on the basis of Article 10(4) of the Europol Decision, Official Journal L 348, p. 1-2 (29 December 2009).

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), Official Journal L 201, p. 37-47 (31 July 2002).

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal L 281, p. 31-50 (23 Novemebr 1995).

Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC (Data Retention Directive). Official Journal L 105, p. 54–63 (13 April 2006).

Directive 2011/92/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA, Official Journal L 335, p. 1-14 (17 December 2011).

Explanations Relating to the Charter of Fundamental Rights, Official Journal C 303, p. 17-35. (14 December 2007).

Proposal for a Directive of the European Parliament and of the Council on Attacks againt Information Systems, replacing Council Framework Decision 2005/222/JHA, 11566/11 (2011).

Regulation 45/2001/EC of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, Official Journal L8 , 1-21 (12.1.2001).

Council Regulation (EC) 881/2002 of 27 May 2002 imposing certain specific restrictive measures directed against certain persons and entities associated with Usama bin Laden, the Al-Qaeda network and the Taliban, and repealing Council Regulation (EC) No 467/2001 prohibiting the export of certain goods and services to Afghanistan, strengthening the flight ban and extending the freeze of funds and other financial resources in respect of the Taliban of Afghanistan, Official Journal L139, p. 9–22 (29 May 2002).

Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, Official Journal L 8, p. 1-22 (12 January 2001).

Regulation (EC) 1987/2006 on the establishment, operation and use of the second generation Schengen Information System (SIS II), Official Journal L 381, p. 4- 23 (28 December 2006).

Regulation (EC) 767/2008 of 9 July 2008 concerning the Visa Information System (VIS) and the Exchange of Data between Member States on Short-stay Visas, Official Journal L 218, p. 60-81 (13 August 2008).

Regulation (EC) 1168/2011 of 25 October 2011 amending Council Regulation No 2007/2004/EC establishing a European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union Official Journal L 304, p. 1-17 (22 November 2011).

7.2.3 Other International Organizations

Drafting Committee on an International Bill of Human Rights (1st session). (1947). *International Bill of Rights Documented Outline* (UN E/CN.4/AC.1/3/ADD.1. Part 1). Retrieved from http://www.un.org/depts/dhl/udhr/docs_1947_1st_draftcom.shtml.

Organization for Economic Cooperation and Development. Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (1980).

United Nations General Assembly (1966). *International Covenant on Civil and Political Rights*, 16 December 1966, Treaty Series, vol. 999, p. 171.

Swedish Parliament, Data Protection Act, 578 (1973 10 May 1973).

7.3 Policy documents

Article 29 Data Protection Working Party. (1998). *Working Document: Transfers of Personal Data to Third Countries: Applying Articles 25 and 26 of the EU data protection directive.* (WP 12). Brussels.

Article 29 Data Protection Working Party. (2004a). *Opinion 4/2004 on the Processing of Personal Data by means of Video Surveillance*. (WP 89). Brussels.

Article 29 Data Protection Working Party. (2004b). *Opinion 9/2004 on a Draft Framework Decision on the storage of data processed and retained for the purpose of providing electronic public communications services or data available in public communications networks with a view to the prevention, investigation, detection and prosecution of criminal acts, including terrorism.* (WP 99). Brussels.

Article 29 Data Protection Working Party. (2005). *Opinion 4/2005 on the Proposal for a Directive of the European Parliament and of the Council on the Retention of Data Processed in Connection with the Provision of Public Electronic Communication Services and Amending Directive 2002/58/EC*. (WP 113). Brussels.

Article 29 Data Protection Working Party. (2006). *Opinion 3/2006 on the Directive 2006/24/EC of the European Parliament and of the Council on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.* (WP 119). Brussels.

Article 29 Data Protection Working Party. (2007). *Opinion N. 4/2007 on the Concept of Personal Data*. (WP 136). Brussels.

Article 29 Data Protection Working Party. (2010a). *Opinion 1/2010 on the Concepts of 'Controller' and 'Processor'*. (WP 169). Brussels.

Article 29 Data Protection Working Party. (2010b). *Opinion 3/2010 on the Principle of Accountability*. (WP 173). Brussels.

Article 29 Data Protection Working Party. (2010c). *Report 01/2010 on the Second Joint Enforcement Action: Compliance at National Level of Telecom Providers and ISPs with the Obligations Required from National Traffic Data Retention Legislation on the Legal Basis of Articles 6 and 9 of the e-Privacy Directive 2002/58/EC and the Data Retention Directive 2006/24/EC Amending the e-Privacy Directive*. (WP 172). Brussels.

Article 29 Data Protection Working Party, and Working Party on Police and Justice. (2009). *The 'Future of Privacy': Joint contribution to the Consultation of the European*

Commission on the Legal Framework for the Fundamental Right to Protection of Personal Data. (WP 168). Brussels.

Bangemann, Martin, et al. (1994). 'Recommendations to the European Council. Europe and the global information society'. The Bangemann Report.

Buttarelli, Giovanni (Assistant EDPS). (2011a). "What future for the Data Retention Directive", speech at the meeting of the EU Council Working Party on Data Protection and Information Exchange (DAPIX - Data Protection), Brussels (4 May 2011).

Buttarelli, Giovanni (Assistant EDPS). (2011b). "Data Protection and security: the Challenges of the Review of the EU legal framework", speaking at the 6th Security Symposium of the European Commission "Security: Old and New challenges", Brussels (20 October 2011).

Buttarelli, Giovanni (Assistant EDPS) (2012). "Latest developments in data protection", presentation at the meeting of the Heads of Agencies, Stockholm (19 October 2012).

Council. (2009). *EU-US High Level Contact Group on data protection and data sharing (HLCG)*.

Council. (2010a). *Draft Internal Security Strategy for the European Union: Towards a European Security Model*. 5842/2/2010. Brussels.

Council. (2010b). *The Stockholm Programme. An Open and Secure Europe Serving and Protecting Citizens*. Official Journal C 115, p. 1–38 (4 May 2010).

European Commission. (1990). *COM (90) 314 final, Directive Concerning The Protection of Individuals in Relation to the Processing of Personal Data, Recommendation for a Council Decision on the Opening of Negotiations With a View to the Accession of the European Communities to the Council of Europe Convention for the Protection of Individuals With Regard to the Automatic Processing of Personal Data, Commission Communication on the Protection of Individuals in Relation to the Processing of Personal Data in the Community and Information Security*. (SYN 287 ns 288). Brussels.

European Commission. (1993). *COM (93) 700, Growth, Competitiveness, Employment. The Challenges and Ways forward into the 21st Century. White Paper*.

European Commission. (2009a). *COM (2009) 342 final, Amended proposal for a Regulation of the European Parliament and of the Council concerning the establishment of 'EURODAC' for the comparison of fingerprints for the effective application of Regulation (EC) No [.../...] [establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person]*. Brussels.

European Commission. (2009b). *COM (2009) 344 final, Proposal for a Council Decision on requesting comparisons with EURODAC data by Member States' law enforcement authorities and Europol for law enforcement purposes*. Brussels.

European Commission. (2010a). *COM (2010) 555 final, Amended proposal for a Regulation of the European Parliament and of the Council on the establishment of 'EURODAC' for the co mparison of fingerprints for the effective application of Regulation (EC) No [.../...] [establishing the criteria and mechanisms for determining the Member State*

responsible for examining an application for international protection lodged in one of th e Member States by a third-country national or a stateless person]. Brussels.

European Commission. (2010b). *COM (2010) 573/4, Strategy for the effective implementation of the Charter of Fundamental Rights by the European Union*.

European Commission. (2010c). *COM (2010) 385 final, Overview of Information Management in the Area of Freedom, Security and Justice*.

European Commission. (2010d). *COM (2010) 492 final, Communication on the global approach to transfers of Passenger Name record (PNR) data to third countries*. Brussels.

European Commission. (2010e). *COM (2010) 673 final, The EU Internal Security Strategy in Action; Five steps towards a more secure Europe*. Brussels.

European Commission. (2011). *COM (2011) 225 final, Report from the Commission to the Council and the European Parliament, Evaluation report on the Data Retention Directive (Directive 2006/24/EC)*. Brussels.

European Commission. (2012a). COM (2012) 10 final, *Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data.*

European Commission. (2012b). *COM (2012) 11 final, Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)*.

European Commission. (2012c). *COM (2012) 254 final, Amended proposal for a Regulation of the European Parliament and of the Council on the establishment of 'EURODAC' for the comparison of fin g erprints for the effective application of Regulation (EU) No [.../...] (establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person) and to request comparisons with EURODAC data by Member States' law enforcement authorities and Europol for law enforcement purposes and amending Regulation (EU) No 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (Recast version)*. Brussels.

European Data Protection Supervisor (EDPS). (2005). *Opinion of 26 September 2005 on the Proposal for a Directive of the European Parliament and of the Council on the retention of data processed in connection with the provision of public electronic communication services and amending Directive 2002/58/EC (COM (2005)438 final)*.

European Data Protection Supervisor (EDPS). (2007). *Opinion of 16 February 2007 on the proposal for a Council Decision establishing the European Police Office (Europol) (COM(2006) 817 final), OJ C 255, 27.10.2007, p. 13*. Brussels.

European Data Protection Supervisor (EDPS). (2009a). *Opinion of 28 July 2009 on the proposal for a Council Regulation amending Regulation (EC) No 881/2002 imposing certain specific restrictive measures directed against certain persons and entities associated with Usama bin Laden, the Al-Qaida network and the Taliban*. Official Journal C 276, p. 1 (17 November 2009).

European Data Protection Supervisor (EDPS). (2009b). *Opinion of 16 December 2009 on various legislative proposals imposing certain specific restrictive measures in respect of Somalia, Zimbabwe, the Democratic Republic of Korea and Guinea.* Official Journal C 73, p. 1 (23 March 2010).

European Data Protection Supervisor (EDPS). (2010a). *Opinion of the European Data Protection Supervisor on the amended proposal for a Regulation of the European Parliament and of the Council concerning the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Regulation (EC) No (.../..) (2010/C 92/01)*. Official Journal C 92, p. 1 (10 April 2010).

European Data Protection Supervisor (EDPS). (2010b). *Opinion of 10 May 2010 on the proposal for a Directive of the European Parliament and of the Council on combating the sexual abuse, sexual exploitation of children and child pornography, repealing Framework Decision 2004/68/JHA*.

European Data Protection Supervisor (EDPS). (2012a). *Opinion of 29 June 2012 on the Communication from the European Commission to the Council and the European Parliament on the establishment of a European Cybercrime Centre*.

European Data Protection Supervisor (EDPS). (2012b). *Opinion of 5 September 2012 on the amended proposal for a Regulation of the European Parliament and of the Council on the establishment of 'EURODAC' for the comparison of fingerprints for the effective application of Regulation (EU) No […/…].*

Hon. Kenneth Younger (Chairman). (1972). *Report of the Committee on Privacy*. London: Her Majesty Stationery Office.

House of Lords. (2009). Surveillance: Citizens and the State (Vol. I: Report). London: Select Committee on the Constitutions.

House of Lords. (2007). Personal internet security- Inquiry. London: Science and Technology Committee.

Hustinx, Peter (EDPS). (2012a). "Data Protection and Schengen Governance" speech delivered at the conference "Upholding Freedom of Movement: an Improved Schengen Governance". Brussels, European Parliament (8 February 2012).

Hustinx, Peter (EDPS) (2012b). "Accountability in the Proposed Regulation", speech given by Peter Hustinx at the IAPP Europe Knowledge Net conference on "Global Trends in Accountability and Getting it Right in the Proposed Regulation", Brussels (3 December 2012).

Meijers Standing Committee of Experts on International Immigration, Refugee and Criminal law. (2009). Note CM0910 on the amended proposal for the Eurodac Regulation (COM (2009) 342) and the Decision on requesting comparisons with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes (COM (2009) 344).

Reding, Viviane (Commissioner). (2011). *The Review of the EU Data Protection Framework, SPEECH/11/183*. Brussels.

Scheinin, Martin. (2009a). *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism*. Geneva: General Assembly.

Swedish Justice Department. (1972). *Data och integritet (Data and Privacy)*. Stockholm: Almänna Förlaget.

United Nations, General Assembly. (1975). *Declaration on the Use of Scientific and Technological Progress in the interest of Peace and for the benefit of Mankind*. (Thirtieth Session, 2400th plenary meeting).

United Nations. *E/CN.4/1028 and Add. 1-3 and Add.3/Corr 1 and Add.4*.

United Nations. (2012). *Human Rights Indicators: A Guide to Measurement and Implementation.* . Retrieved from http://www.ohchr.org/Documents/Publications/Human_rights_indicators_en.pdf.

United Nations Office on Drug and Crime (UNODC). (2012). The Use of Internet for Terrorist Purposes. Vienna: United Nations.

US Department of Defense. (2008). GPS Navstar, Global Positioning System Standard Positioning service performance standard.

7.4 Case law

7.4.1 European Union

Advocate General Léger. (2005). *Opinion on Cases C-317&04 and C318/04*.

Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v Netlog NV, C-360/10. Judgment of the Court (Third Chamber) of 16 February 2012.

Commission v. Austria, C-614/10.Judgment of the Court (Grand Chamber). Judgment of the Court (Eighth Chamber) of 24 May 2012.

Commission v Council, C-440/05. Judgment of the Court (Grand Chamber) of 23 October 2007.

Germany v Council, C-426/93. Judgment of the Court of 9 November 1995.

Ireland v European Parliament and Council, C-301/06,. Judgment of the Court (Grand Chamber) of 10 February 2009.

Kadi and Al Barakaat International Foundation v Council and Commission (Kadi I), Joined Cases C-402/05 P and C-415/05. Judgment of the Court (Grand Chamber) of 3 September 2008.

Karlsson and Others, C-292/97. Reference for a preliminary ruling, Judgment of the Court (Sixth Chamber) of 13 April 2000.

Nold KG v Commission, C-4/73. Judgment of the Court of 14 May 1974.

Parliament v. Council and Commission (PNR cases), Joined Cases C-317/04 and C-318/04. Judgment of the Court (Grand Chamber) of 30 May 2006.

Parliament v Council, C-355/10. Judgment of the Court (Grand Chamber) of 5 September 2012.

Reference for a preliminary ruling from High Court of Ireland in the case Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources, Minister

for Justice, Equality and Law Reform, The Commissioner of the Garda Síochána, Ireland and the Attorney General (2012), C-293/12.

Tietosuojavaltuutettu v Satakunnan Markkinapörssi Oy and Satamedia Oy, C-73/07. Judgment of the Court (Grand Chamber) of 16 December 2008.

Volker und Markus Schecke GbR and Hartmut Eifert v. Land of Hesse, Joined Cases C-92/09 and C-93/09. Judgment of the Court (Grand Chamber) of 9 November 2010.

Wachauf V Bundesamt Für Ernährung Und Forstwirtschaft, C-5/88. Judgment of the Court (Third Chamber) of 13 July 1989.

7.4.2 European Court of Human Rights

Amann v. Switzerland, No. 27798/95 (2000).

Bouchacourt v. France, No. 5335/06 (2009).

Gillan and Quinton v. United Kingdom, No. 4158/05 (2010).

Glor v. Switzerland, No. 13444/04 (2009).

Guzzardi v. Italy, No. 7367/76 (1980).

Iordachi v. Moldova, No. 25198/02 (2009).

Klass v. Germany No. 5029/71 (1977).

Kopp v. Switzerland, No. 23224/94 (1998).

Kvasnica v. Slovakia, No. 72094/01 (2009).

Liberty and others v. United Kingdom, No. 58243/00 (2008).

Malone v. United Kingdom, No. 8691/79 (1984).

Nada v. Switzerland, No. 10593/08 (2012).

Peck v. United Kingdom, No. 44647/98 (2003).

Perry v. United Kingdom, No. 63737/00 (2003).

S and Marper v. United Kingdom, No. 30562/04 (2008).

Uzun v. Germany (2010).

Weber and Saravia vs. Germany, No. 54934/00 (2006).

7.4.3 Human Rights Committee

Human Rights Committee. (1988). *General Comment No. 16.* Geneva.

Human Rights Committee. (1999). *General Comment No. 27*. Geneva.

Human Rights Committee. (2004). *General Comment No. 31, The Nature of the General Legal Obligation.* Geneva.

Human Rights Committee. (2006) Sayadi and Vinck v. Belgium, 1472/2006.

Human Rights Committee. (2007). *General comment No. 32, Right to equality before courts and tribunals and to a fair trial*. Geneva.

Human Rights Committee. (2011). *General comment No. 34, Freedoms of opinion and expression.* Geneva.

7.4.4 Other Judicial Bodies

Bundesverfassungsgericht (German Federal Constitutional Court). BVerfGE 65. 1 - Volkszaehlung Urteil des Ersten Senats vom 15 Dezember 1983 auf die muendlliche Verhandlung vom 18. und 19. Oktober 1983- I BvR 209.269. 362.420.440.484/83 in dem Verfahren ueber die Verfassungsbeschwerden (1983).

____. 1 BvR 2074/05 and 1 BvR 1254/07 (2008).

____. 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08 (2011).

Center for Democracy & Technology, Electronic Frontier Foundation, Matt Blaze, Andrew J. Blumberg, Roger L. Easton and Norman M. Sadeh. (2011). Amicus Brief in support of respondent in United States v. Jones.

Czech Republic Constitutional Court. (2011). Judgment 24/10, No. 94/2011 Coll.

International Court of Justice. (2004). *Advisory Opinions on the Legal Consequences of a Wall in the Occupied Palestinian Territory*.

Romanian Constitutional Court. (2009). Decision no. 1258 Regarding the unconstitutionality exception of the provisions of Law no.298/2008 regarding the retention of the data generated or processed by the public electronic communications service providers or public network providers, as well as for the modification of law 506/2004 regarding the personal data processing and protection of private life in the field of electronic communication area.

Supreme Court of Ireland. (2010). Digital Rights Ireland limited vs. the Minister for Communication, Marine, and Natural Reource, the Minister of Justice, Equality and Law Reform, the Commissioner of an Garda Siochana, Ireland and the Attorney General, No. 3785/P.

United States v. Jones, Justice Sotomayor concurring opinion, No. 565 U.S. (U.S. Supreme Court 2012).

Verfassungsgerichtshofes Oesterreich. (2012). Constitutional Court has reservations against data retention and turns to the CJEU, from http://www.vfgh.gv.at/cms/vfgh-site/attachments/2/7/9/CH0003/CMS1355817745350/press_release_data_retention.pdf.