Project acronym:	PRISMS
Project title:	The PRIvacy and Security MirrorS: Towards a European framework for integrated decision making
Project number:	285399
Programme:	Seventh Framework Programme for research and technological development
Objective:	SEC-2011.6.5-2: The relationship between Human privacy and security
Contract type:	Collaborative project
Start date of project:	01 February 2012
Duration:	42 months

Deliverable 5.3: The legal significance of individual choices and the relation between security, privacy and personal data protection

Authors:	Gloria González Fuster, Serge Gutwirth (VUB)
Reviewer:	Dara Hallinan (Fraunhofer ISI)

Dissemination level:	Public
Deliverable type:	Report
Version:	1.0
Due date:	31 March 2014
Submission date:	20 February 2015

About the PRISMS project

The PRISMS project analyses the traditional trade-off model between privacy and security and devise a more evidence-based perspective for reconciling privacy and security, trust and concern. It examines how technologies aimed at enhancing security are subjecting citizens to an increasing amount of surveillance and, in many cases, causing infringements of privacy and fundamental rights. It conducts both a multidisciplinary inquiry into the concepts of privacy and security and their relationships and an EU-wide survey to determine whether people evaluate the introduction of security technologies in terms of a trade-off. As a result, the project determines the factors that affect public assessment of the security and privacy implications of a given security technology. The project uses these results to devise a decision support system providing users (those who deploy and operate security systems) insight into the pros and cons, constraints and limits of specific security investments compared to alternatives taking into account a wider society context.

Terms of use

This document was developed within the PRISMS project (see http://prismsproject.eu), co-funded by the European Commission within the Seventh Framework Programme (FP7), by a consortium, consisting of the following partners:

- Fraunhofer Institute for Systems and Innovation Research (Fraunhofer ISI), co-ordinator,
- Trilateral Research & Consulting LLP,
- Dutch Organization for Applied Scientific Research (TNO),
- Vrije Universiteit Brussel (VUB),
- University of Edinburgh (UEdin),
- Eőtvős Károly Policy Institute (EKINT),
- Hogeschool Zuyd and
- Market & Opinion Research International Limited (Ipsos-MORI)

Document history

Version	Date	Changes
1.0	20 February 2015	

Contents

Pamiętajcie, cena, którą płacić trzeba za wolność, maleje, gdy rośnie popyt.
(*Don't forget: the price to be paid for freedom gets diminished according to the demand*).[1]

Stanisław Jerzy Lec, 1957

1 INTRODUCTION

This report investigates the legal significance of individual choices for defining the relation between security, privacy and personal data protection. It constitutes a reflexive deliverable aiming to contribute to the interpretation of the findings of the Privacy and Security Mirrors (PRISMS)[2] research project by throwing light on the role that law grants to personal preferences in those matters.

'Law' is primarily understood here as what judges and courts do whenever they rule, rather than legislation.[3] The present deliverable is thus particularly concerned with how legal decisions are taken using or ignoring individual choices related to security, privacy and personal data protection. As such, it does not aim to directly investigate whether (and how) decision makers might take these individual preferences into account when defining related security, technology or research policies,[4] or when legislating.[5] The report will nonetheless, when appropriate, delineate the background of relevant discussions, refer to how positive law sometimes appears to integrate the consideration of individual choices.

As an opening reflection, it must be recalled that whenever policy makers in the European Union (EU) take security-related decisions they have the obligation to ensure that these are compliant with fundamental rights requirements, and they might also, additionally, be interested in questioning whether individuals would actually perceive such decisions as impacting fundamental rights negatively or not.[6] These are two different issues that cannot be conflated, as one strictly regards compliance with fundamental rights, while the other is about perceptions of compliance. The respect of fundamental rights is unquestionably a legal issue, while perceptions of compliance might be described as a societal consideration, often addressed from an economic perspective and in terms of their possible negative impact on the commer-

[1] Translation courtesy of Dariusz Kloza.
[2] For more information, http://prismsproject.eu/.
[3] On the specificity of law in this field, see: González Fuster, Gloria and Serge Gutwirth, "Ethics, Law and Privacy: Disentangling Law from Ethics in Privacy Discourse", in *Proceedings of the 2014 IEEE International Symposium on Ethics in Science, Technology and Engineering, 23-24 May 2014, Chicago*, IEEE, 2014.
[4] On the relation between public debate and technological research, for instance, see: von Schomberg, René, "Introduction: Towards Responsible Research and Innovation in the Information and Communication Technologies and Security Technologies Fields'", in von Schomberg, René (ed.), *Towards Responsible Research and Innovation in the Information and Communication Technologies and Security Technologies Fields*, Publications Office of the European Union, Luxembourg, 2011, [p. 13].
[5] On the use of public opinion shifts to support decisions by policy makers, see, for instance: Potoglou, Dimitris, N. Robinson, C. W. Kim, et al., "Quantifying individuals' trade-offs between privacy, liberty and security: the case of rail travel in UK", *Transportation Research Part A: Policy and Practice*, Vol. 44, No. 3, 2010, pp. 169-181, [p. 170].
[6] The importance of this concern is notably developed in: European Commission, "Commission Staff Working Paper: Security Industrial Policy, Security Industrial Policy Accompanying the Document Communication from the Commission to the European Parliament, the Council and the European Economic and Social Committee Security Industrial Policy Action Plan for an Innovative and Competitive Security Industry {COM(2012) 417 Final}", SWD(2012) 233 Final, Brussels, 2012. See for instance p. 11 referring to public fear provoked by some security measures, or p. 28 stating that security technologies are often perceived as an intrusion of the personal sphere.

cialisation of technological products.[7] This report is certainly not about the latter, but rather about investigating how legal compliance as such, as determined by judges and courts, proceeds to take into account individual choices referring to security, privacy and personal data protection.

Individual choices might manifest themselves independently, as a single, personal choice, or in conjunction with other individual preferences. In this case, a sum of individual choices can take the shape of a perceived public opinion, or at least of a certain public opinion, that is, representing the opinion of a certain public. This report takes into consideration these two possibilities, and gives particular attention to situations in which the endorsement of the choices of some individuals might appear to be in conflict with the choices of other individuals.

From a conceptual viewpoint, individual choices can be regarded as both reflecting and informing individual preferences. When related to the right to respect for private life and personal data protection, individual choices and preferences might be pictured as globally subsumed under the term 'privacy concerns'. In this contexts, it is necessary to keep in mind that individual actions and decisions related to privacy and personal data protection are always multidimensional, and sometimes inconsistent and contradictory.[8] These 'privacy concerns' include attitudinal aspects, related to what people perceive, feel and think; cognitive aspects, related to what people know and the information they are provided; and practical or behavioural aspects, related to what people do, particularly in the cases where choice is actually effectively in their hands.[9] All these dimensions are of course interrelated, and influence each other.

A telling example of a case where ignorance of the issues at stake seems to directly affect practical decisions taken by individuals on privacy-related issues can be found in the context of fingerprinting of migrants in application of EU laws. The European Commission has observed that in some cases migrants which should be fingerprinted in accordance with applicable laws do not receive from competent authorities a clear explanation of this fact and of the legal consequences linked to their possible refusal. As a result, some of the uninformed migrants decide to refuse being fingerprinted without knowing that, in the cases where they have not yet applied for asylum, their refusal could be treated as an indication that they are likely to abscond, and become an argument used to justify their detention.[10]

The present report starts with an examination of the principles guiding the relation between fundamental rights and individual choices. This section is followed by a study of the significance of individual choices for the adjudication of the right to respect for private life, firstly, and for the adjudication and regulation of the right to personal data protection, secondly. Fi-

[7] In this sense, ibid., p. 28.
[8] Muñoz Soro, José Félix and Daniel Oliver-Lalana, *Derecho y cultura de protección de datos: Un estudio sobre la privacidad en Aragón*, Dykinson, Madrid, 2012, [p. 41].
[9] Oliver-Lalana, Daniel and José Félix Muñoz Soro, "El mito del consentimiento y el fracaso del modelo individualista de protección de datos", in Valero Torrijos, Julián (ed.), *La protección de los datos personales en Internet ante la innovación tecnológica: Riesgos, amenazas y respuestas desde la perspectiva jurídica*, Aranzadi, Cizur Menor, 2013, [p. 169]. On the limits of gathering knowledge on these dimensions, see for instance: Szoka, Berin, "Privacy Polls v. Real-World Trade-Offs", Progress Snapshot, The Progress & Freedom Foundation, 2009.
[10] European Commission, "Report from the Commission to the European Parliament and the Council: Fifth Bi-Annual Report on the Functioning of the Schengen Area 1 November 2013 - 30 April 2014", COM(2014) 292 final, Brussels, 2014, [p. 4].

nally, the report discusses some of the key tensions in the taking into account of individual choices in modern EU personal data protection law.

2 GENERAL PRINCIPLES OF FUNDAMENTAL RIGHTS PROTECTION

As described in PRISMS Deliverable 5.2,[11] in the EU the relationship between security, privacy and personal data protection is most critically played out at the level of fundamental rights. It seems thus necessary to open up the present reflection on the legal significance of individual choices in this area with some insights related to the very notion of fundamental rights.

2.1 RIGHTS OF ALL

Fundamental and human rights aim to protect everybody. They are precisely recognised as such because they are considered to be rights of the highest value in the legal orders that enshrine them, and they are rights to which all individuals are entitled. In the system of the Council of Europe, this idea is clearly documented by the fact that the European Convention on Human Rights (ECHR) systematically refers to 'everyone' as the subject of the rights established by its provisions: for example, Article 8 of the ECHR, on the right to respect for private and family life, states that '[e]veryone *has the right to respect for his private and family life, his home and his correspondence'*. Article 34 of the ECHR, mirroring this approach, sets out that 'any person' might file an application before the European Court of Human Rights (ECtHR) claiming to be the victim of a violation of the rights set forth in the Convention. In a similar vein, the Charter of Fundamental Rights of the EU also asserts in its Article 7 that *everyone* has the right to respect for his or her private and family life, home and communications, and its Article 8(1) establishes that *everyone* has the right to the protection of personal data concerning him or her.

The fact that everybody is entitled to the enjoyment of fundamental rights directly implies that those rights are not only destined to protect the majority of individuals, but also any possible minorities. If somebody's choices are in conflict with those of the majority, this cannot result in depriving them of protection. On the contrary, typically it will be precisely those whose personal choices differ from the choices of the majority who will be in particular need of claiming and exercising their fundamental rights and freedoms. In this sense, the majority can be described as being 'naturally' preserved by the very social strength of its own normality; 'normal persons', by their very condition of being normalised, enjoy a sort of shelter that people living marginal lives, dissidents and minorities in general simply lack.[12]

Translated into the specific area of the relationship between security, privacy and personal data protection this notably entails that the right to privacy and to personal data protection must aim to protect everybody as opposed to just people with normal or average 'privacy concerns'. Actually, it is probably those with singular and extra-ordinary 'privacy concerns' that will be in particular need of legal protection, and it is also for them that they should be effective.

[11] González Fuster, Gloria, Serge Gutwirth, Bernadette Somody, et al., "Consolidated legal report on the relationship between security, privacy and personal data protection in EU law", PRISMS Deliverable 5.2, 2014.
[12] Díez-Picazo, Luis María, *Sistema de derechos fundamentales*, Aranzadi, Cizur Menor (Navarra), 2013, [p. 57].

2.2 RIGHTS PROTECTED WITH SPECIAL SAFEGUARDS

Fundamental and human rights are typically given an especially high status in European legal orders, status which aims to preserve them from some of the oscillations of the will of the majority as represented and enacted by the legislator. This special rank is also derived from the human rights obligations originating in the ratification of international treaties and agreements, such as the ECHR. In the EU, Member States sometimes condition the adoption of norms restricting the exercise of fundamental rights and freedoms to special legislative requirements, and might provide for reinforced judicial control whenever fundamental rights are at stake. This will mean, for instance, that legal norms formally backed up by the legislator might be declared null and void by the judiciary due to a violation of constitutionally protected rights and freedoms.

This shielding of fundamental rights and freedoms from the will of the majority is grounded on an acknowledgement of the fact that, in practice, rights of minorities are often violated with the majority's explicit or implicit approval. But the shielding must also be linked to another basic feature of fundamental rights, which is their dual dimension as being regarded by law as valuable both subjectively and objectively.[13] If fundamental rights have a subjective dimension insofar as they aim to protect concrete individuals, they also have an objective dimension in the sense that they are regarded as foundational elements of constitutional democratic states. And, because of this objective dimension, they must be insured and promoted by public authorities regardless of the eventual particular preferences of some (or many) individuals.

2.3 LIMITED POSSIBILITIES OF WAIVER

Another attribute derived from the basic premise according to which fundamental and human rights are recognised as being of the greatest importance for the legal order establishing them is that, in principle, individuals cannot generally relinquish them. It would be paradoxical for any legal order to place at its summit a selected set of rights and freedoms, envisioned as subjectively and objectively essential, and then to confer to individuals the possibility to just renounce to them on the basis of their personal choices. Establishing a general possibility to relinquish fundamental and human rights could be understood as an indication that the legal order in question accepts that giving away a series of guarantees that it simultaneously claims to be essential. A general renouncing to fundamental and human rights, or even to specific rights or freedoms, shall thus be regarded as inadmissible. Individuals cannot, for instance, decide to renounce their personal freedom and accept slavery, or to give up their freedom of expression and condemn themselves to eternal silence.[14]

This does not mean, however, that individuals are obliged to exercise their fundamental rights and freedoms in all cases and under all circumstances. In point of fact, the exercise of these rights and freedoms can never be imposed on them. Individuals might choose to refrain from reacting to a violation of any of their rights. The prohibition of a global waiver of fundamental rights coexists with the recognition of individual freedom, and thus law attempts to strike a

[13] Ibid., p. 55.
[14] Ibid., p. 137

balance between the autonomy of the individual and the State's obligation to protect fundamental rights.[15]

The major implication of the prohibition of general waiver of rights is that any exercise of a fundamental right must be considered legitimate and valid regardless of any possible previous commitment stating that a right would not be used.[16] Individuals must always remain free to decide to exercise their rights, and thus any general statement in an opposite sense is to be treated as legally inconsequential. What could happen, nonetheless, is that, by first announcing that they renounce to the exercise of a right and later deciding to still exercise it, individuals generate negative consequences for a third, and thus such a decision could, in certain cases, be subject to compensation.

Another important limitation of the waiver of fundamental rights is that it is never possible to relinquish their exercise in favour of the State: public authorities cannot impose, support or accept a waiver of this kind, which would go against one of the basic functions of fundamental rights in general, which is to limit the power of public authorities.[17] This is particularly pertinent in relation to the right to respect for private life, commonly envisaged as located at the very heart of individual freedom and concretely aiming to ensure individuals to be free from arbitrary state interference. The right's classical conception as devising an abstract space that the State cannot penetrate would be in full contradiction with granting to the State the possibility to put any kind of pressure on individuals to surrender this protection.

[15] For a discussion of the issue of waiver in these terms, see: Schutter, Olivier De, *International human rights law: Cases, materials, commentary*, Cambridge University Press, Cambridge, United Kingdom, 2014, [pp. 498ff.].
[16] Díez-Picazo, 2013, [p. 139].
[17] Ibid., p. 138.

3 INDIVIDUAL CHOICES IN THE ADJUDICATION OF PRIVACY

After the above general review of existing knowledge on fundamental rights and the legal significance of individual choices, this Section examines how individual choices operate specifically in the adjudication of the right to respect for private life. It focuses on the case law of the ECtHR on Article 8 of the ECHR, and gives particular attention to the insights that could illuminate the importance of individual choices for defining the relationship between security, privacy and personal data protection.

ECtHR's case law is especially appropriate for this task due to the Strasbourg's Court's emphasis on the need to interpret the ECHR in a dynamic way, also taking into account changes in social attitudes.[18] The ECtHR famously stressed in 1978 that the European Convention is '*a living instrument'* that '*must be interpreted in the light of present-day conditions'*,[19] and has for instance concluded that Article 8 of the ECHR encompasses an obligation not to discriminate against children born out of wedlock after observing that laws in the great majority of Member States of the Council Europe had evolved and were evolving in such direction.[20]

3.1 INDIVIDUAL PERCEPTIONS AND THE SCOPE OF PRIVATE LIFE

One of the ways in which individual choices can play a role in the adjudication related to the right to respect for private life is by affecting the construction of the notion of 'private life', which has never been defined or thoroughly circumscribed by the ECtHR.[21] Delimiting the contours of 'private life' is decisive to determine the scope of Article 8 of the ECHR.

Generally speaking, law can approach the delimitation of this notion in two distinct ways, either by granting a wide discretion to individuals to decide what they wish to keep protected under such a term, or rather by following material criteria able to reach a conclusion on whether something should be protected or not regardless of the particular wishes of the individual affected.[22] From the first perspective, what people want to keep private, is what is to be viewed as private; from the second, what shall be protected as private can and should be delimited on the basis of objective factors without considering individual wishes. To follow the first perspective can be problematic both in the cases where individuals do not wish to have any protection at all, despite the objective dimension of the right, and in situations where they aspire to too extensive protection.

The ECtHR has generally considered that what needs to be protected under the right to respect for private life cannot vary completely from one person to another merely depending on their personal wishes, and that there is a certain minimum to be necessarily protected to ensure individuals' dignity and quality of life. The Court has stressed that 'private life' must be understood as a broad term, encompassing a zone of interaction with others, even in a public context.[23] And it has put forward a number of elements to be taken into account to determine

[18] Harris, D. J., M. O'Boyle, Ed Bates, et al. (eds.), *Law of the European Convention on Human Rights*, Oxford University Press, Oxford, United Kingdom, 2014.
[19] *Tyrer v UK*, Judgment of the Court (Chamber), of 25 April 1978, § 31.
[20] *Marckx v. Belgium*, Judgment of the Court (Plenary) of 13 June 1979, § 61.
[21] Harris, et al. (eds.), 2014.
[22] Díez-Picazo, 2013, [p. 281].
[23] See, for instance, *Uzun v Germany,* judgment of the Court (Fifth Section) of 2 September 2010, § 43 and case law cited thereof.

if a person's private life is affected when people are outside their home or private premises, such as the systematic or permanent record of information about individuals.[24]

The Strasbourg Court has repeatedly detached itself from the so-called 'expectations of privacy' doctrine. This doctrine, imported from the United States (US), conditions the existence of a violation of somebody's privacy to the requirement that the individual in question was actually legitimately expecting to enjoy privacy protection. The Court has observed that, in order to determine whether a measure constitutes an interference with the right to respect for private life, a person's reasonable expectations as to privacy may be a significant, but not necessarily conclusive, factor.[25] The ECtHR, therefore, does not condition the recognition of an interference with the right to respect for private life to the fact that the individual had actually any concrete expectations of privacy. The Court, nonetheless, sometimes takes into account whether actions such as the publication of recorded material occurs in a manner or degree that goes beyond what was normally foreseeable; if that is the case, this can be considered as an important element to regard the action as falling under the scope of the right to respect for private life.[26]

All in all, it can be deduced there is no need to prove the existence of a general expectation of privacy in a concrete circumstance to actually be granted the right to obtain privacy protection. Nevertheless, individuals' expectations in terms of anticipated limited use of personal information can be an important factor to determine whether there has been an interference with their fundamental rights. The Court, therefore, appears to grant only a limited significance to individual choices in those matters, preferring to rely on objective criteria to determine the possible existence of interferences with the right to respect for private life under Article 8 of the ECHR.

Also in relation to other rights set out by the ECHR, the Strasbourg Court has been reluctant to grant any major relevance to societal views for the determination of the scope of the right protected. For instance, in 1978 the Strasbourg Court observed that the fact that birching of young persons had many advantages according to the local public opinion of the Isle of Man was irrelevant to the question whether such birching constituted inhuman and degrading treatment.[27]

3.2 CAN PUBLIC PERCEPTIONS LEGITIMISE INTERFERENCES?

A different issue is whether some public perceptions or choices can play a role in the legitimisation of interferences with the rights of the ECHR, and concretely with the right to respect for private life of its Article 8. This right is one of those enshrined in the ECHR that might be legitimately limited in certain circumstances and in accordance with certain requirements. When considering applications of individuals who claim their rights under Article 8 of the ECHR have been violated, the Strasbourg Court first examines whether the applicant's rights have been affected, and, if an interference is indeed established, it then turns to the question of whether the restriction can be regarded as permissible.

[24] *P.G. and J.H. v. the UK*, judgment of the Court (Third Section) of 25 September 2001, § 57.
[25] Idem.
[26] *Uzun* § 48.
[27] *Tyrer*, § 38.

To be permissible, restrictions of the rights contained in Article 8 of the ECHR must be 'necessary in a democratic society' for achieving one of the aims listed in the Article's second paragraph.[28] Among these aims stands out the pursuance of 'national security' and security-related objectives such as the prevention of disorder or crime, which are notions that the Court has however never defined through the lens of public or individual perceptions of what might constitute security, or disorder, or crime.

The ECtHR has held that the requirement of being 'necessary in a democratic society' does not mean that measures constituting interferences must be 'absolutely necessary' or 'indispensable', but it has equally underlined that it is not enough for measures to be merely 'useful' or 'desirable'.[29] In the Court's view, for an interference to be 'necessary in a democratic society' it must correspond to a 'pressing social need'. The requirement of amounting to a 'pressing social need', however, does not imply that interferences must be approved the majority of society. Two important judgments throw light on the role granted to public perceptions for the possible justification of interferences with the rights protected under Article 8 of the ECHR.

The first, *Dudgeon v UK,* dates from 1981 and was about the criminalisation of male homosexual acts in Northern Ireland.[30] In this case, the ECtHR pointed out that this prohibition concerned a most intimate aspect of private life, and, therefore, it could only be justified on the grounds of particularly serious reasons. The Strasbourg Court argued that some forms of legislation could be regarded as '*necessary*' to protect particular societal groups and '*the moral ethos of society as a whole'*, but added that any measures needed nevertheless to remain within the bounds of what might be regarded as strictly necessary to accomplish the aims pursued.[31] The Court noted that it was '*relevant'*, in order to assess compliance with the requirements of Article 8(2) of the ECHR on the legitimacy of interferences, to examine *'the moral climate in Northern Ireland in sexual matters'*, which encompassed '*a genuine and sincere conviction shared by a large number of responsible members of the Northern Irish community that a change in the law would be seriously damaging to the moral fabric of society'*.[32] These elements, however relevant, were nevertheless not sufficient according to the Court to justify the maintenance in force of the impugned legislation insofar as it had the general effect of criminalising private homosexual relations between adult males capable of valid consent.[33] Indeed, they did not amount by themselves to a proof that there was a '*pressing social need'* to make such male homosexual acts criminal offences.[34] In this context, the Court also noted that the 'democratic society' to which alludes the requirement of being 'necessary in a democratic society' bears as hallmarks tolerance and broadmindedness.[35]

In the second judgment, *Smith and Grady v UK*, of 1999, the ECtHR addressed the investigation into and subsequent discharge of personnel from the armed forces on the basis of their homosexuality.[36] Here, the Court notably made explicit that the measures at stake could not

[28] That is, 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 (Art. 8(2) of the ECHR).
[29] See notably *Handyside v the UK,* Judgment of the Court (Plenary) of 7 December 1976, § 48.
[30] *Dudgeon v UK*, Judgment of the Court (Plenary) of 22 October 1981.
[31] *Dudgeon*, § 49.
[32] Ibid., § 57.
[33] *Dudgeon*, § 61.
[34] Ibid., § 60.
[35] Ibid., § 53.
[36] *Smith and Grady v UK,* Judgment of the Court (Third Section) of 27 September 1999.

be justified on the basis of social negative attitudes towards homosexuals. In its defence, the UK government had put forward a report allegedly expressing the general views of the personnel on the issue, but the Court described such report as documenting negative attitudes of heterosexual personnel towards those of homosexual orientation which '*ranged from stereotypical expressions of hostility* […] *to vague expressions of unease about the presence of homosexual colleagues'*.[37] The Court added that, to the extent that these negative attitudes expressed '*a predisposed bias'*, they could not be considered to amount to sufficient justification for the interferences with the applicants' '*any more than similar negative attitudes towards those of a different race, origin or colour'*.[38] Doing so, the ECtHR unambiguously declared simply irrelevant for the justification of interferences with Convention rights these categories of negative attitudes.

[37] Ibid., § 97.
[38] Idem.

4 INDIVIDUAL CHOICES AND EUROPEAN PERSONAL DATA PROTECTION

PRISMS Deliverable 5.2 described personal data protection as a hinge with the capacity to act as an interface between security and privacy, facilitating the balancing between them. It is thus particularly important to understand which role individual choices play in this interface.

Entering the discussion of the relation between personal data protection and individual choices, here construed widely as involving also individual attitudes, knowledge and practices, there are a few general observations that can be advanced. First of all, it must noted that the EU legislator often appears to rely on a vision of individuals as 'data subjects', that is, as subjects of the right to personal data protection, that are poorly informed and prone to take wrong decisions.[39] This vision is sometimes illustrated by the image of individuals that are confused up to the point of ignoring that the services that they use, and that they imagine to be free services, are as a matter of fact services that they are actually paying for, not with money but through the provision of their own personal data.

This viewpoint contrasts but coexists with a second perspective, according to which data subjects are nevertheless in a position to decide freely on whether they should consent or not to certain personal data processing practices, at least in some circumstances. This idea is firmly entrenched in EU personal data protection, through the notion of consent.

4.1 THE ROLE OF CONSENT

In the current EU personal data protection legal landscape, individual consent can operate as one of the grounds rendering personal data processing activities lawful.[40] The provision of the Charter of Fundamental Rights of the EU on the right to personal data protection, Article 8, explicitly refers to consent by establishing that personal 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'*.[41] The explicit reference to consent made in this provision actually concedes to this ground a symbolically privileged position among all possible legitimate basis for personal data processing.

Consent can operate as a legitimate basis for personal data processing only in some circumstances, as for it to be valid data subjects must have been given a genuine and free choice and be subsequently able to refuse or withdraw consent without detriment. Despite this limitation, through the notion of consent EU personal data protection law appears to grant great relevance to individual choices. If the major exception to the validity of consent is indeed that it shall not be valid when individuals have no real choices, this could be seen as implying that whenever they do have a choice, their choice should be taken into account.

[39] On this issue, see notably: González Fuster, Gloria, "How uninformed is the average data subject? A quest for benchmarks in EU personal data protection", *IDP Revista de Internet, Derecho y Política*, No. 19, 2014, pp. 92-104.

[40] This is the general function of consent of EU personal data protection law. It also plays other roles, notably as a means to render lawful the processing of sensitive data, generally prohibited (for this purpose, consent shall be explicit), and consent can also render lawful data transfers to third countries that would be otherwise not allowed.

[41] Art. 8(2) of the Charter of Fundamental Rights.

In practice, however, there has been much discussion in the literature about whether consent, as it functions in everyday situations, actually reflects the true choices of individuals or is performing independently or against such choices.[42] It must be stressed that in order to be valid, consent must formally be informed, which means that data subjects should have been appropriately informed about the specific purposes of the data processing operations to which they consent. Nevertheless, it is questionable whether in light of the general misinformed condition of data subjects, as hinted above, and despite any punctual information provided to them, they can be regarded as being informed enough as to provide fully informed consent.

The widespread use of consent as a legitimising basis for personal data processing activities and its known problems can lead one to think that, instead of allowing to express and enforce individual choices, it rather ends up covering a waiver to any real possibility of effective control. This has notably led the consideration of the doctrine of consent as a myth.[43] Despite these criticisms, the legislative package for the review of EU personal data protection law introduced in 2012 by the European Commission[44] confirms and reinforces the prominence of consent, supported as contributing to the 'empowerment' of data subjects.[45]

The case law of the Court of Justice of the EU (CJEU) offers some insights on the significance of individual choices in EU personal data protection law, and in particular in relation to consent. The most important judgment in this area is *Deutsche Telekom*,[46] of 2011, concerning the obligation placed on an undertaking assigning telephone numbers to pass to other undertakings data in its possession relating to the subscribers of third-party undertakings. In this ruling, the Luxembourg Court examined a provision of Directive 2002/58/EC[47] giving to subscribers of telecommunication services the opportunity to determine whether their personal data shall be included in public directories.[48] The Court declared that this provision did not grant to subscribers a selective right to decide in favour of certain providers: by consenting to have their data being published in a directory with a specific purpose, individuals lose standing to object to the publication of the same data in another, similar directory.[49]

The judgment in *Deutsche Telekom* is revealing insofar as it appears to grant to individual choices a real impact, but an impact nevertheless limited in scope. Individuals might accept or refuse a processing of personal data (in that specific case, the publication of personal data in a directory), but cannot decide who shall be responsible for such processing (they cannot accept

[42] Oliver-Lalana and Muñoz Soro, 2013, [p. 160]. On consent in EU personal data protection, see also: Kosta, Eleni, *Consent in European data protection law*, Martinus Nijhoff Publishers, Leiden, 2013.
[43] Oliver-Lalana and Muñoz Soro, 2013, [. 167].
[44] European Commission, "Safeguarding Privacy in a Connected World: A European Data Protection Framework for the 21st Century", COM(2012) 9 final, Brussels, 2012. European Commission, "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)", COM(2012) 11 final, Brussels, 2012; European Commission, "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 offencesor the execution of criminal penalties, and the free movement of such data", COM(2012) 10 final, Brussels, 2012.
[45] Oliver-Lalana and Muñoz Soro, 2013, [p. 164].
[46] Case C-543/09 *Deutsche Telekom AG v Bundesrepublik Deutschland*, Judgment of the Court (Third Chamber) of 5 May 2011.
[47] "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 of the European Communities L 201*, Vol. 45, 31 July 2002, pp. 37-47.
[48] Art. 12(2) of Directive 2002/58/EC.
[49] *Deutsche Telekom,* § 62.

for the processing only on the condition that it takes place under the control of a certain company, and oppose to it if it is carried out by another).

Other judgments of the CJEU provide generally only glimpses of knowledge on the role that consent is supposed to play in EU personal data protection law. A particularly puzzling example is the ruling in *Volker und Markus Schecke and Eifert*, of 2010.[50] In this case, the Luxembourg Court dismissed the possibility that the processing of personal data at stake (namely, the online publication of beneficiaries of EU funds) was grounded on consent, noting that it was based instead on a legal obligation, and concluding from this fact that there had been an interference with the EU fundamental right to personal data protection that had to comply with the requirements of limitations imposed by the horizontal provisions of the EU Charter.[51] What is striking, however, is that the Court appeared to treat consent as a possible way not only to legitimise personal data processing as such, but rather as a means to actually set aside the possibility that an interference with the EU fundamental right to the protection of personal data ex Article 8 of the EU Charter had taken place at all.[52] This could be read as implying, *a contrario*, that whenever data subjects have consented to a particular data processing operation, the operation cannot be regarded as an interference with their fundamental right to personal data processing.[53]

4.2 CHOOSING BETWEEN INDIVIDUAL CHOICES AND THE PUBLIC INTEREST

There is however still another noteworthy judgment of the CJEU on the legal significance of individual choices for EU personal data protection. This ruling, *Google Spain*, of 2014,[54] concerns more concretely the possible tensions between a particular individual choice and the potential interest of the public in opposing such choice. The CJEU addressed indeed the issue of whether data subjects have a right to request that any list of results displayed following a search made on the basis of their name does not display some information relating to them that is inadequate, irrelevant or no longer relevant. The Court asserted that data subjects have indeed such a right, in the light of Articles 7 and 8 of the EU Charter, and underlined that as a general rule this right overrides the right of the general public in having access to that information upon a search relating to the data subject's name.[55]

This dominant role granted to the individual choice to have some information removed from a list of results in front of the potential public preference to have the information preserved is, nevertheless, not asserted with a general character, but rather as a presumption that might be contested and invalidated. The Luxembourg Court observes in this sense that the overriding of the right of the general public in having access to the information upon the search on the data subject's name can in some cases not take place, if special conditions apply. That would be the case, the Court notes, if it appeared that for particular reasons, such as the role played by the data subject in public life, the interference with their fundamental rights is justified by the

[50] Joined Cases C-92/09 and C-93/09, Judgment of the Court (Grand Chamber) of 9 November 2010, *Volker und Markus Schecke GbR (C-92/09) and Hartmut Eifert (C-93/09) v Land Hessen*, 2010 I-11063.
[51] See notably § 62 and 63.
[52] See § 61 and § 64.
[53] On the weaknesses of existing CJEU case law on the right to personal data protection, see notably González Fuster, Gloria, "Fighting For Your Right to What Exactly? The Convoluted Case Law of the EU Court of Justice on Privacy and/or Personal Data Protection", *Birkbeck Law Review*, Vol. 2, No. 2, 2014, pp. 263-278.
[54] Case C-131/12, *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González*, Judgment of the Court (Grand Chamber) of 13 May 2014.
[55] *Google Spain*, § 97.

preponderant interest of the general public in having, on account of inclusion in the list of results, access to the information in question.[56]

4.3 THE VIEWS OF DATA SUBJECTS IN DATA PROTECTION IMPACT ASSESSMENTS

Another way in which EU personal data protection law might integrate in the future the taking into account of individual choices is through the regulation of 'data protection impact assessments'. The General Data Protection Regulation proposed by the European Commission in 2012 foresees indeed establishing the obligation to carry out 'data protection impact assessments' in certain circumstances. Concretely, according to the proposed text, in the future wherever processing operations present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes, the controller or the processor acting on the controller's behalf shall carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.[57] In the context of this assessment, the data controller shall take into account '*the rights and legitimate interests of data subjects and other persons concerned',* as stated in Article 33(3) of the proposed General Data Protection Regulation, and *'shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of the processing operations'*, as detailed in Article 33(4).

It is unclear at the moment whether these provisions will effectively see the light in those exact terms when (and if) the proposed General Data Protection Regulation is adopted. What can be observed already, in any case, is that there is much vagueness as to how the data controller shall take the rights and interests of data subjects *'and other persons concerned'* into account. It is similarly obscure why, if the data controllers have to take into account the views of both data subjects *'and other persons concerned'*, they shall only seek the views of the former.

[56] Idem.
[57] Art. 33(1) of the proposed General Data Protection Regulation.

5 CONCLUDING THOUGHTS

This report has shown that, legally speaking, the significance of individual choices for defining the relation between security, privacy and personal data protection has multiple facets. Globally speaking, law appears to be ready to fully support personal choices, even those choices that go against of the choices of other individuals, however numerous or persuasive the latter are. It will, for example, decide to ignore some societal opinions that are perceived as going against the basic principles of inclusiveness of democratic societies. Law can also, nonetheless, pursue the protection of individuals also against their own individual choices, and for this purpose reduce or limit the relevance of their preferences.

Against this complex background, the role granted to consent by EU personal data protection law strikes as particularly ambiguous. This ambiguity can manifest in concrete individual decisions, where single acts of consent might appear to go against some established knowledge on the limitations on the waiver of rights. More remarkably, the widespread use and misuse of consent as a ground to process personal data in the EU can also have global consequences when the fact that many individuals appear to 'consent' to some popular data processing practices, for instance via the active use of online social media, is taken as evidence of their preferences or lack of 'privacy concerns'. In a similar vein, policy makers appear to have an increased interest in attempting to appraise the economic value of personal data in the eyes of data subjects, in the understanding that such examination could provide orientation for future policy decision in this area.

In face of these developments, it is crucial to go back to the idea of the multidimensionality of privacy concerns, and to rethink how the limitations imposed by law on the significance of individual choices can be appropriately integrated into their construal. As previously noted, attitudes, knowledge and practices related to privacy and personal data protection cannot be envisaged as independent dimensions, because they affect each other. From this viewpoint, one should not focus on trying to assess or calculate individuals' 'personal' preferences in relation to the use of personal data concerning them, or to merely take note of how lightly people appear to consent to certain data processing practices, but rather investigate the factors that determine such preferences and practices.[58] In other words, instead of acting as if there were some pre-existing personal choices that happen to operate among the current legal landscape for privacy and personal data protection, it might be necessary to inquiry how the current legal landscape shapes current attitudes and decisions, and, finally, discuss which kind of preferences and choices should it encourage or discourage.[59] The exact legal significance of these choices will afterwards, in any case, shift (back) to the hands of courts and judges.

[58] Rouvroy, Antoinette, "Réinventer l'art d'oublier et de se faire oublier dans la société de l'information?", in Lacour, Stéphanie (ed.), *La sécurité de l'individu numérisé. Réflexions prospectives et internationales*, L'Harmattan, Paris, 2008, [p. 16].
[59] Ibid., p. 17

BIBLIOGRAPHY

Díez-Picazo, Luis María, *Sistema de derechos fundamentales*, Aranzadi, Cizur Menor (Navarra), 2013.

"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 of the European Communities* L 201, Vol. 45, 31 July 2002, pp. 37-47. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:201:0037:0047:EN:PDF

European Commission, "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 offencesor the execution of criminal penalties, and the free movement of such data", COM(2012) 10 final, Brussels, 2012a.

European Commission, "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)", COM(2012) 11 final, Brussels, 2012b.

European Commission, "Safeguarding Privacy in a Connected World: A European Data Protection Framework for the 21st Century", COM(2012) 9 final, Brussels, 2012c.

European Commission, "Commission Staff Working Paper: Security Industrial Policy, Security Industrial Policy Accompanying the Document Communication from the Commission to the European Parliament, the Council and the European Economic and Social Committee Security Industrial Policy Action Plan for an Innovative and Competitive Security Industry {COM(2012) 417 Final}", SWD(2012) 233 Final, Brussels, 2012d.

European Commission, "Report from the Commission to the European Parliament and the Council: Fifth Bi-Annual Report on the Functioning of the Schengen Area 1 November 2013 - 30 April 2014", COM(2014) 292 final, Brussels, 2014.

González Fuster, Gloria, "How uninformed is the average data subject? A quest for benchmarks in EU personal data protection", *IDP Revista de Internet, Derecho y Política*, No. 19, 2014, pp. 92-104. http://edcp.uoc.edu/proceedings_idp2014.pdf

González Fuster, Gloria, and Serge Gutwirth, "Ethics, Law and Privacy: Disentangling Law from Ethics in Privacy Discourse", in *Proceedings of the 2014 IEEE International Symposium on Ethics in Science, Technology and Engineering, 23-24 May 2014, Chicago*, IEEE, 2014, pp. 1-6.

González Fuster, Gloria, Serge Gutwirth, Bernadette Somody, and Ivan Székely, "Consolidated legal report on the relationship between security, privacy and personal data protection in EU law", PRISMS Deliverable 5.2, 2014.

González Fuster, Gloria, "Fighting For Your Right to What Exactly? The Convoluted Case Law of the EU Court of Justice on Privacy and/or Personal Data Protection", *Birkbeck Law Review*, Vol. 2, No. 2, 2014, pp. 263-278. http://www.bbklr.org/2-2-6.html

Harris, D. J., M. O'Boyle, Ed Bates, and Carla Buckley (eds.), *Law of the European Convention on Human Rights*, Oxford University Press, Oxford, United Kingdom, 2014.

Kosta, Eleni, *Consent in European data protection law*, Martinus Nijhoff Publishers, Leiden, 2013.

Muñoz Soro, José Félix , and Daniel Oliver-Lalana, *Derecho y cultura de protección de datos: Un estudio sobre la privacidad en Aragón*, Dykinson, Madrid, 2012.

Oliver-Lalana, Daniel , and José Félix Muñoz Soro, "El mito del consentimiento y el fracaso del modelo individualista de protección de datos", in Julián Valero Torrijos (ed.), *La protección de los datos personales en Internet ante la innovación tecnológica: Riesgos, amenazas y respuestas desde la perspectiva jurídica*, Aranzadi, Cizur Menor, 2013, pp. 153–196.

Potoglou, Dimitris, N. Robinson, C. W. Kim, P. Burge, and R. Warnes, "Quantifying individuals' trade-offs between privacy, liberty and security: the case of rail travel in UK", *Transportation Research Part A: Policy and Practice*, Vol. 44, No. 3, 2010, pp. 169-181.

Rouvroy, Antoinette, "Réinventer l'art d'oublier et de se faire oublier dans la société de l'information?", in Stéphanie Lacour (ed.), *La sécurité de l'individu numérisé. Réflexions prospectives et internationales*, L'Harmattan, Paris, 2008, pp. 249-278. http://works.bepress.com/antoinette_rouvroy/5/ (Extended version)

von Schomberg, René, "Introduction: Towards Responsible Research and Innovation in the Information and Communication Technologies and Security Technologies Fields'", in René von Schomberg (ed.), *Towards Responsible Research and Innovation in the Information and Communication Technologies and Security Technologies Fields*, Publications Office of the European Union, Luxembourg, 2011, pp. 7-15. http://ec.europa.eu/research/science-society/document_library/pdf_06/mep-rapport-2011_en.pdf

Schutter, Olivier De, *International human rights law: Cases, materials, commentary*, Cambridge University Press, Cambridge, United Kingdom, 2014.

Szoka, Berin, "Privacy Polls v. Real-World Trade-Offs", Progress Snapshot, The Progress & Freedom Foundation, 2009. http://www.pff.org/issues-pubs/ps/2009/pdf/ps5.10-privacy-polls-tradeoffs.pdf

Co-ordinator:
Dr. Michael Friedewald
Fraunhofer Institute for Systems and Innovation Research ISI
Breslauer Straße 48 | 76139 Karlsruhe | Germany
Phone: +49 721 6809-146 | Fax +49 721 6809-315
michael.friedewald@isi.fraunhofer.de