The Future of EU Working Parties' "The Future of Privacy" and the Principle of Privacy by Design

By Ugo Pagallo and Eleonora Bassi

1. Introduction

It is not hard to understand why there are so many current publications on "the future of," say, science, law and technology, the internet, the public domain, etc. [Hugenholtz & Guibault, 2006; Zittrain, 2008; Brockman, 2009; Fernández-Barrera *et al.*, 2009; Brockman, 2010]. Whether or not you admit that we are in the midst of an "information revolution" [Bynum 2009, Horner 2010], technology is profoundly changing how we live, think, and interact. Scholars are eager to unfold the ideas that will be setting the trend in five or ten years, along with the innovations that could radically transform our entire world.

Consider the case of current legal systems and how technology affects them: While the study of this impact should not be blind to the reciprocal interaction between technology and society, we can fully grasp this transformation in three ways.

First, technology has deeply changed the approach of experts to legal information.

Secondly, technology has induced new kinds of lawsuits or has modified old forms.

Thirdly, technology has blurred traditional national boundaries as information on the internet tends to have a ubiquitous nature.

Such a threefold impact, however, has made some scholars adopt a sort of techno-deterministic stance, according to which there would be no way to shape or, at least, to influence the evolution of technology. Think about data protection and the reasons why some have announced "The End of Privacy" [Sykes, 1999], "The Death of Privacy in the 21st Century" [Jarfinkel, 2000], or "Privacy Lost" [Holtzmann, 2006]. Technology is what allows these scholars to unveil an already written future: In the digital environment, data protection would simply vanish due to the use of spyware, root-kits, profiling techniques, data mining, not to mention FBI programs like Carnivore or Magic Lantern. In everyday (or analog) life, some means like RFID, GPS, CCTV, AmI, or satellites, would lead to the same effect.

More recently, researchers pushed the issue even further by envisaging a world where we will read people's thoughts from the signals emitted by their brains: "It will be the ultimate invasion of privacy" [Ford, 2010]. Likewise, other scholars imagine that solid-state memory will replace hard drives and we will live with pervasive computational presence: Of course, "battery size remains a barrier to progress, but this will improve, along with increased efficiency of our electronics (…). Privacy will vanish" [Garrett Lisi, 2010].

Yet, rumours of the death of privacy may have been greatly exaggerated and, what is more, these techno-deterministic approaches are liable to the criticism that John Kenneth Galbraith put forward in his own field: "The only function of economic forecasting is to make astrology look respectable." Therefore, in dealing with "the future of privacy," this paper does not rely on prophetic powers or divinatory commitments: Rather, the aim is to draw attention to some major issues of today's data protection laws by examining the joint contribution of the EU Article 29 Data Protection Working Party (WP29) and the Working Party on Police and Justice (WPPJ). The document "The Future of Privacy" (02356/09/EN – WP168) adopted on December 1st, 2009, allows us to highlight crucial problems involving data protection today as well as to specify possible developments and changes induced by technology.

The paper is presented in three sections.

First, we examine how data protection is changing by focusing on some of the topics considered by the European WPs. Besides the need for a new legal framework in terms of globalisation and

international standards, binding corporate rules and accountability, the European WPs pay special attention to technological changes and "Privacy by Design as a new principle." In a nutshell, the formula implies that data protection should be "embedded" in ICT through default settings, enabling business, public sector, as well as individuals to "take relevant security measures by themselves."
Secondly, we look at some highly debatable conclusions of EU WPs, namely, matters of jurisdiction on the internet. If we admit that cookies amount to 'equipment' pursuant to art. 4(1)c of Directive 95/46/EC, we end up in a paradox: According to WPs's opinion, if a US citizen is accessing a US web site during the 3rd ISIL-meeting in Corfu, the enforceable norms are the laws on data protection in the EU!
Thirdly, we stress some remarkable silences in the WPs's document on "The Future of Privacy." Along with DNA data and biometrics, such silences concern the EU Directive 2003/98/EC on the processing and re-use of the public sector information (PSI). This is telling because the rules adopted by the EU legislator aim to overcome some barriers limiting the re-use of PSI, while subordinating such re-use to the provisions on the protection of personal data. Once the goal is to create or promote added-value services with macro-economic relevance – like what we find in the U.S. nowadays – we need to prevent the risk that today's information society refrains from re-use of PSI in Europe, due to the potential liability deriving from privacy protection.
Such a problem suggests that we deepen the "new principle" of privacy by design. The ubiquitous nature of the internet, in fact, does not only transcend traditional legal borders – thereby prompting EU WPs to admit that "global standards regarding data protection are becoming indispensable" – because the internet also questions the notion of the law as made up of commands enforced through physical sanctions. By allowing business, public sector, and individuals to take "relevant security measures by themselves," the new approach of "privacy by design" reformulates the enforcement of data protection as a matter of "restricted access" and "limited control" [Tavani, 2007].

2. A sketch of the future

EU WPs's document on "The Future of Privacy" focuses on five main points, namely, i) the need for a new comprehensive legal framework; ii) technological changes and privacy by design as an innovative principle; iii) the empowering of data subjects; iv) the strengthening of data controllers' responsibility; v) stronger and clearer roles for Data Protection Authorities (DPAs), and their cooperation within the EU. Although the central message of the document "is that the main principles of data protection are still valid despite the new technologies and globalisation," the document stresses that we need to clarify some key rules and principles of the legal framework, such as consent and transparency, so as to introduce further principles in order to strengthen the effectiveness of the system.
The reason making this integration necessary depends on the restructuring of the EU institutions following the Lisbon Treaty that entered into force on December 1st, 2009. The former division between pillars have been replaced by a new horizontal approach to data protection and privacy pursuant to art. 16 of the Treaty on the Functioning of the European Union (TFEU).
However, there is a further reason for reshaping the current legal framework: It depends on the very evolution of the internet. According to the U.S. President's principal advisors on telecommunications and information policy – that is, both the National Telecommunications and Information Administration (NTIA), and the Assistant Secretary of Commerce for Communications and Information, Lawrence Strickling – we need an "Internet Policy 3.0 (…) to respond to all the social changes being driven by the growth of the Internet." More particularly, in the case of data protection, the issue can be summarized in the following way: "How can we enable the development of innovative new services and applications that will make intensive use of personal information but at the same time protect users against harm and unwanted intrusion into their privacy?" [Strickling, 2010]

Hence, in order to strike a fair balance between people's privacy and, say, "the development of innovative new services and applications" like social network services or cloud computing, let us have a closer look at these five main points, according to which the EU WPs's document on "The Future of Privacy" addresses the general subject of today's data protection.

2.1 A comprehensive legal framework

There are two peculiarities of EU law on data protection [Pagallo, 2008].
The first distinctive feature concerns the aim to ensure a "general and harmonized protection" of people's privacy within the 27 Member States of the Union: For instance, in the U.S., the Supreme Court has declared that "the protection of a person's general right to privacy [is] left largely to the law of the individual States" [Katz v. U.S., 389 U.S. 347, 350-51 (1967)]. In the European Union, the Court of Justice has affirmed that all Member States have the duty to implement the general standard of protection established by the European directives [C-101/01, Lindqvist case, § 96].
The second peculiarity involves the aim of the law, *i.e.*, why EU legal system aims to guarantee such a "general protection." While it is debatable whether or not a property standpoint prevails in the U.S. [Lessig, 2002; Volkman, 2003], it is pretty clear that data protection is considered as an autonomous fundamental right in Europe. In the opinion of the German Constitutional Court, both the confidentiality and integrity of information technology systems represent basic constitutional rights of the individual [BVG's Judgement from February 27th, 2008, 1 BvR 370/07; 1 BvR 595/07].
Following these premises, the EU WPs have declared in the document on "The Future of Privacy" that both key notions and main principles of the Directive 95/46/EC on data protection should be deemed the "backbone" of a more comprehensive legal network. This does not mean that some of these concepts need not be clarified as in the case of "consent" and "transparency" (see below 2.3). Besides, it does not follow that some innovations are unnecessary: The WPs think it is crucial to enhance the level of data protection through specific regulations, in accordance with the general principles of "privacy by design" (upon which *infra* 2.2), and of accountability (2.4). Among the specific issues put forward by the document, we find national security policy, police and judicial cooperation, security breaches, privacy tools and services such as seals and audits. Further detailed regulations would be necessary for a number of sectors like public health, employment, and intelligent transport systems.
However, the document admits that it would be meaningless to set up this comprehensive legal framework, without considering trends of globalisation: "Even though the individual often lives a local life, he can more and more be found on line where his data are processed globally. Globalisation therefore is linked to technology, the position of the data subject, data controller, DPAs/WP29 and law enforcement."
Accordingly, we need to take into account current technological changes in order to ensure the general protection of people's personal data through a more comprehensive legal framework. After all, the WPs recall that basic concepts of the first European directive on data protection (D-95/46/EC) developed in a world where information processing was characterized by "card index boxes, punch cards and mainframe computers."

2.2 Technological changes and privacy by design

The idea of embedding data protection safeguards in ICT is not totally new. While art. 17 of D-95/46/EC lays down the obligation of data controllers to implement appropriate technical and organizational measures, recital 46 of the same European directive requires that such measures have to be taken "both at the time of the design of the processing system and at the time of the processing itself, particularly in order to maintain security and thereby to prevent any unauthorized processing."

In the late 1990s, the concept of "Privacy by Design" was further developed by the Ontario's Privacy Commissioner, Ann Cavoukian, to cope with the "ever-growing and systemic effects" of both ICT and large-scale networked data systems. In April 2000, a working paper on "Privacy Design Principles for an Integrated Justice System" was jointly presented by the Ontario's Privacy Commissioner and the U.S. Department of Justice [Cavoukian, 2009].
Yet, at least in Europe, the EU WPs admit that the provisions of the Directive have been insufficient and, therefore, "the new legal framework has to include a provision translating the currently punctual requirements into a broader and consistent principle of privacy by design. This principle should be binding for technology designers and producers as well as for data controllers who have to decide on the acquisition and use of ICT."
More specifically, the EU WPs single out some of the goals that should be reached, *e.g.*, data minimization and quality of the data, together with its controllability, transparency, confidentiality, and user friendliness of information interfaces. Among the examples of how the new principle can contribute to better data protection, the EU WPs recommend that biometric identifiers "should be stored in devices under control of the data subjects (i.e., smart cards) rather than in external data bases." In addition, the EU WPs suggest that making personal data anonymous both in public transportation systems and in hospitals should be considered a priority. In the first case, video surveillance must be designed in such a way that faces of individuals cannot be recognizable; in hospitals' information systems, patient names should be kept separated from data on medical treatments and health status.
Besides the proposals of the EU WPs, the idea of incorporating data protection safeguards in ICT has been discussed by scholars as, for instance, in the recent "Intelligent Privacy Management Symposium" at Stanford University, CA., on March 22nd-24th, 2010 [the program is online at http://research.it.uts.edu.au/magic/privacy2010/]. Moreover, in section 4, we further examine why the principle of privacy by design is particularly relevant when examining the implementation of the European directive on the re-use of PSI.
For the moment, it suffices to recall what the EU WPs claim in the light of the abovementioned recital 46 of the European directive on data protection, namely, that the principle of privacy by design should be applied "as early as possible." This seems indeed to be another case where prevention is better than cure.

2.3 Empowering the data subjects

Individuals' rights to data protection must go hand in hand with the obligations for the entities that process personal data. Among the main individuals' rights we find open access to personal data, the ability to modify and to delete that data, and the right to refuse at any given time to have such data processed. Among the main obligations of the data controllers, there is the duty of processing personal data fairly and lawfully, by informing the individuals so as to gain their consent when required by the law. Furthermore, data controllers must protect the processing with security measures and filing processing with local public authorities pursuant to recital 25 of the Directive 95/46/EC.
In the opinion of EU WPs, however, current technological developments have profoundly impacted on this legal framework, so that changes in the behaviour and role of the data subjects require strengthening the position of the individuals. The document on "The Future of Privacy" stresses five points.
First, there is the need of improving redress mechanisms with the introduction of class actions procedures which already exist in the EU environmental law.
Secondly, transparency is a pre-requisite for individuals to give their valid consent. Along with new ways to inform data subjects in relation to behavioural advertising, a general privacy breach notification should be introduced in the new legal framework.

Thirdly, it is apparent that technological developments require a careful consideration of consent because, especially on the internet, implicit agreement does not always mean unambiguous consent. In the words of the U.S. Assistant Secretary of Commerce for Communications and Information, "more and more personal data was being collected leading to a growing unease with the 'notice & choice' model. How many of us really read those privacy policies or just click away at the 'Yes, I agree…' in order to get on with what you want to buy, read or post?" [Strickling, 2010]
Fourthly, there is a problem of harmonisation: The interpretation of the EU data protection laws is now and then inconsistent and many Member States have implemented neither the liability provision nor the possibility to claim non-economic damages set up by the Directive from 1995.
Finally, a lack of safeguards surrounds the ever-growing number of cases involving the individuals who upload their own personal data onto the internet, *e.g.*, via online social networks or cloud computing services. For instance, the creation of pre-built profiles of non-members through the aggregation of data, which is independently contributed by the users of social network services, lacks a legal basis or, perhaps worse, leads to incongruous outcomes. It is sufficient to recall what the Article 29 Data Protection Working Party denounced in its Opinion 5 from June 2009 (01189/09/EN WP 163): "Even if the SNS [social network service] had the means to contact the non-user and inform this non-user about the existence of personal data relating to him/her, a possible e-mail invitation to join the SNS in order to access these personal data would violate the prohibition laid down in Article 13.4 of the ePrivacy Directive [*i.e.*, D-2002/58/EC] on the sending of unsolicited electronic messages for direct marketing purposes."

2.4 Strengthening the responsibility of data controllers

Dealing with the main obligations of data controllers (see above 2.3), the EU WPs regret that "compliance with existing legal obligations often is not properly embedded in the internal practices of organizations." The effectiveness of the provisions of D-95/46/EC thus require a number of pro-active measures: Data controllers should adopt internal policies and processes, while defining the mechanisms in order to execute them. Moreover, organizations should draft compliance reports and carry out audits and privacy impact assessments, so as to obtain third-party certifications or seals.
Yet, the document on "The Future of Privacy" warns that "Web 2.0 services and cloud computing are blurring the distinction between data controllers, processors and data subjects." In its Opinion the 1st of February 2010 on the very concepts of "controller" and "processor" (00264/10/EN WP 169), the WP29 remarks that "the concept of controller is a functional concept, intended to allocate responsibilities where the factual influence is, and thus based on a factual rather than a formal analysis. Therefore, determining control may sometimes require an in-depth and lengthy investigation."
Nevertheless, many doubts persist despite such an in-depth and lengthy investigation. Consider the twelfth example of the abovementioned WP29's Opinion 5/2009 on social networks: "Social network service providers provide online communication platforms which enable individuals to publish and exchange information with other users. These service providers are data controllers, since they determine both the purposes and the means of the processing of such information."
Hence, would a SNS be responsible for damages caused by its users' uploading data?
While many legal systems, among which the U.S. federal law, provide for safe harbours or limitations on liability for the internet intermediaries in the case of unlawful users' conduct or user-generated content, the situation is far from clear in Europe [Pagallo, 2009].
On one side, an Italian Court admitted the responsibility of the internet providers when sentencing some of Google's executives in the Vividown suit for allowing a video to be posted online showing an autistic youth being abused [Tribunal of Milan, decision 1972 from February 24th, 2010].
According to the ECJ decision on March 23rd, 2010, in *Google v. Louis Vitton* (case 236/08), "in order to establish whether the liability of a referencing service provider may be limited under Article 14 of Directive 2000/31, it is necessary to examine whether the role played by that service

provider is neutral, in the sense that its conduct is merely technical, automatic and passive, pointing to a lack of knowledge or control of the data which it stores" (§ 114 of the decision). In other words, it as all about "the actual terms on which the service in the cases in the main proceedings is supplied," so that the Court of Paris should "assess whether the role thus played by Google corresponds to that described in paragraph 114 of the present judgment" (*ibid.*, § 117).
On the other side, the aforementioned WP29's Opinion on social networks suggests how the liability of SNS should be grasped: SNS are only obliged to provide information and adequate warning to users about privacy risks when uploading data, so that "users should be advised by SNS that pictures or information about other individuals, should only be uploaded with the individual's consent" [see also Sartor & Viola, 2010].
Therefore, at the end of the day, what do we really mean by strengthening the responsibility of data controllers? Do we want data controllers to be obliged to monitor the network in an unprecedented and perhaps unmanageable manner? Does art. 15 of the EU Directive 2000/31/EC on e-commerce rule out this duty, in that "Member States shall not impose a general obligation on providers, when providing the services covered by Articles 12, 13 and 14, to monitor the information which they transmit or store, nor a general obligation to actively seek facts or circumstances indicating illegal activity"?
Moreover, what about matters of jurisdiction between, say, EU and U.S.? Are today's standard international legal approaches sufficient or should we look for alternative ways in coping with global privacy issues?
In order to further clarify some of these questions, let us proceed with the analysis of "The Future of Privacy": The WPs's remarks on both the role and functions of the European authorities on data protection allow us to straighten on some of these problems.

2.5 The role of the authorities

The fifth (and final) issue examined by the EU WPs's document on "The Future of Privacy" concerns the role of the Data Protection Authorities (DPAs). The subject is particularly relevant for three reasons.
First, notwithstanding the limits on which we insist below, EU DPAs' role has been altogether positive, specially when you compare it with the functioning of the U.S. Privacy and Civil Liberties Oversight Board under the Bush administration. To sum the point up with the Director of the ACLU's Technology and Liberty Program, Barry Steinhardt, "when it comes to how we handle privacy, America should be moving toward Europe – not forcing them to move toward us" (Steinhardt's statement from February 2nd, 2004, is online at http://www.aclu.org/technology-and-liberty/new-report-shows-why-americans-must-join-europeans-protect-privacy-aclu-says).
Secondly, despite this positive record, the role of DPAs can be improved. As stressed by the EU WPs's Opinion, there are still big differences regarding the position of DPAs in the twenty seven Member States of the Union, while art. 28 (1) of D-95/46/EC is unclear with regard to their true independence.
Similarly, a new legal framework should include both DPAs's power to impose financial sanctions on controllers and processors, and their role as a consultative body in future legislation on data protection. Taking into account changing contexts within the EU, changing emphasis in law enforcement and unmet challenges for data protection such as data mining, intelligent CCTVs, biometric tools, and the risk of growing inaccuracies, *e.g.*, cases of false negatives- and false positives-subjects, the thesis of the EU WPs's document is that "cooperation between DPAs in charge of ensuring lawfulness of data processing should be strengthened in all matters and integrated in the legal framework, also by envisaging stable mechanisms (…) in order to foster a harmonised approach across the EU and beyond."
Finally, the role of DPAs brings us back to matters of enforceability and jurisdiction. As mentioned above (see supra 2.1), data protection is a fundamental right under EU law, so that, in the opinion of

the WPs, "the EU and its Member States should guarantee this fundamental right for everybody, in so far as they have jurisdiction. In a globalised world, this means that individuals can claim protection also if their data are processed outside the European Union."
However, the same document recalls the indispensability of global standards and the necessity of international agreements for the protection of personal data in today's context. The document on "The Future of Privacy" singles out specific forms of international and even of transnational cooperation such as the Binding Corporate Rules (BCRs), *i.e.*, international codes of conduct for multinationals in order to regulate the worldwide transfer of data.
Thus, let us clarify how there may be a problematic divergence between the harmonization of law-making within the EU and the call for international cooperation. A good example of such a divergence is the case of transnational cookies.

3. Transnational cookies

Before we illustrate the EU WPs's Opinion on the legal status of cookies, that is, the file-texts put on your computer's hard disk by a web site when you are accessing it, we need to define what 'transnational' law really means. By comparing this adjective with the more frequent term of 'international' law – in all likelihood coined by Jeremy Bentham – some basic Latin helps.
On one hand, 'inter' means 'between' or 'in-between.' According to the standard Westphalian model, international law is in fact the law between sovereign nation-states and not, say, between their citizens or subjects. As stressed by Jack Goldsmith, the (traditional) idea is that "in the absence of consensual international solutions, prevailing concepts of territorial sovereignty permit a nation to regulate the local effects of extraterritorial conduct" [Goldsmith, 1998].
On the other hand, 'trans' means 'beyond' so that transnational law implies something that lays beyond nation-states and their control, *i.e.*, it is entwined with international law but does not coincide with it. One of the first occasions when the formula was used, is Philip Jessup's characterization of transnational law as "all law which regulates actions or events that transcend national frontiers. Both public and private international law are included, as are other rules which do not wholly fit into such standard categories" [Jessup, 1956].
More than half a century later, the "other rules" of Jessup's definition of transnational law may be summed up in accordance with the multiple fields where this idea "has proven most fruitful and provocative" [Zumbansen, 2008]: Think about *lex mercatoria*, corporate governance, public international law, human rights litigation, and even transnational citizenship [Bauböck, 1994]. In this category, we should add the realm of ICT law and the cyberspace, on which the EU WPs have been focusing in several Opinions and other contributions mentioned here. Following David Post's critique of Goldsmith's traditional ideas on international law, information technology has produced "a world in which virtually all events and transactions have border-crossing effects" and, therefore, such "effects and transactions, previously at the margins of the legal system and of sufficient rarity to be cabined off into a small corner of the legal universe (…) have migrated, in cyberspace, to the core of that system" [Post, 2002].
Consequently, when examining some typical cross-border effects of cyberspace, *e.g.*, jurisdictional issues of personal data protection, what law applies? Is it the law of the sovereign national state which disciplines the local effects of extraterritorial conduct or the "other rules" of transnational law? More particularly, when an EU citizen is accessing a web site whose equipment is located outside the EU, are the EU laws on data protection enforceable?
In the next section (3.1), we examine the thesis put forward by the EU Article 29 Data Protection Working Party since its Opinion from May 30th, 2002 (5035/01/EN/Final WP 56).
Then (3.2), we illustrate some flaws in the thesis.
Finally (3.3), an alternative way to approach the issue is suggested.

3.1 EU laws in cyberspace

In the aforementioned document from 2002, the WP29 declared the EU law to be applicable, when a "US web site puts a cookie on the personal computer of individuals in the EU in order to identify the PC to the web site in view of linking up that information with others." There are two reasons why:
First of all, in accordance with the thesis on the principle of sovereignty and "a nation's right to control events within its territory" [Goldsmith, 1998], the WP29 claimed that "a survey of international law suggests that States have a tendency to use several alternative criteria for determining extensively the scope of application of national law" (see again Document 5035/01/WP56). Specifically, the criterion adopted by the WP was that 'equipment' included cookies pursuant to art. 4 (1)c of D-95/46/EC: "Each Member State shall apply the national provisions it adopts pursuant to this Directive to the processing of personal data when (…) the controller is not established on Community territory and, for purposes of processing personal data, makes use of equipment, automated or otherwise, situated on the territory of the said Member State."
Secondly, the WP29 argued that the aim is not only to extend the range of applicability of EU law but, rather, to ensure the protection of people's rights: "The objective of this provision in Article 4 paragraph 1 lit. c) of Directive 95/46/EC is that an individual should not be without protection as regards processing taking place within his country, solely because the controller is not established on Community territory. This could be simply, because the controller has, in principle, nothing to do with the Community. But it is also imaginable that controllers locate their establishment outside the EU in order to bypass the application of EU law."
(More recently, as we mention in section 2.5, the EU WPs's document on "The Future of Privacy" admits that "article 4 of the directive, determining when the directive is applicable to data processing, leaves room for different interpretation." Nevertheless, in accordance with the previous opinion from May 30th, 2002, they insist that the protection of people's fundamental rights "means that individuals can claim protection also if their data are processed outside the European Union.")
Of course, one could rebut the twofold argument of the WP29's document, by observing that, from a historical perspective, the protection of fundamental rights questions the idea of the law being based upon the principle of sovereignty. Moreover, in the case of cyberspace, we should add that "all conduct has geographically far-flung effects on people and institutions around the world" so that "there will continually be conflicts between a principle that permits sovereigns to regulate on the basis of those effects, and a principle that sovereigns can only regulate where they have the consent of the regulated" [Post, 2002].
Still, there are more pragmatic reasons for considering the EU WP's reasoning weak. They concern the legislation of every single Member State of the EU and how foreign companies could exclude EU users from their services. Let us examine more carefully some of these criticisms.

3.2 Pan-jurisdiction and its paradoxes

Scholars often stress why it is wrong to hold cookies to be an 'equipment' pursuant to art. 4 (1)c of D-95/46/EC. In this context, it is enough to mention five reasons.
First, among the definitions of art. 2 of D-95/46/EC, 'equipment' is not legally defined: To consider cookies as a sort of equipment would be more a matter of political choice than of legal interpretation.
Secondly, many EU provisions apply to non-European companies doing business in Europe: This entails evident issues in the field of consumer law for instance. Many of these companies have thus trouble excluding EU users from their services, in that such companies, in order to do so, would need to establish residence and name of such users, which clearly entails potential infringements on data protection and other issues of jurisdiction: Ultimately, this leads to a vicious circle.

Thirdly, by considering cookies as an 'equipment', the principal criterion according to which EU Member States should apply the directive would not hinge on the place where the data controller is established. Rather, contrarily to the rationale of the directive, its applicability would depend on the emplacement of the data subject.
Fourthly, by applying EU data protection laws to all the websites using cookies on the internet, foreign data controllers would be compelled to simultaneously comply with the legislation of every single Member State of the EU, which raises an "impossible burden" [Kuner, 2003].
Fifthly, there is the paradox mentioned in the introduction of this paper. Once you admit that cookies constitute an 'equipment', it follows that every time a US citizen is accessing a US website during, say, a holiday in Europe, the enforceable norms would be the EU laws on data protection.
In the light of these and other possible shortcomings, are there alternative ways to deal with the drawbacks of the EU jurisdiction?

3.3 Feasible way outs

In his Opinion from July 25th, 2007 (2007/C 255/01), the European Data Protection Supervisor (EDPS), Peter Hustinx, recalled the ECJ decision of the Linqvist case (see above 2.1), in order to warn how "this system, a logical and necessary consequence of the territorial limitations of the European Union, will not provide full protection to the European data subject in a networked society where physical borders lose importance (…): the information on the Internet has an ubiquitous nature, but the jurisdiction of the European legislator is not ubiquitous."
In fact, cyberspace issues, like other cases put forward by contemporary *lex mercatoria*, corporate governance, or human rights litigation, show the limits of current international approaches based upon the principle of sovereignty and the nations' right to unilaterally control events within their territories. As proposed by Peter Hustinx in the aforementioned Opinion, the challenge of protecting personal data on the international level "will be to find practical solutions" through typical transnational measures such as "the use of binding corporate rules by multinational companies" and "international agreements on jurisdiction." Furthermore, there is the need of "promoting private enforcement of data protection principles through self-regulation and competition," while "accepted standards such as the OECD-guidelines for data protection (1980) and UN-Guidelines could be used as basis."
Quite significantly, this is also what the EU WPs have somehow proposed in "The Future of Privacy," when remarking the importance of both international agreements and codes of conduct for multinationals, together with global standards regarding data protection (see above 2.5).
Besides, global issues of data protection could be effectively analyzed through EU WPs's "idea of incorporating technological protection safeguards in information and communication technologies," *i.e.*, according to the principle of privacy by design, which "should be binding for technology designers and producers as well as for data controllers who have to decide on the acquisition and use of ICT" (see supra 2.2).
So, in order to further illustrate how the principle may function, let us introduce this new topic of design and the field of personal data protection: Even though the EU WPs have not examined the subject matter in their Opinion, the realm of the public sector information (PSI) helps us shed new light on "The Future of Privacy."

4. The troubles with the public sector information

Silence can be more telling than words. It is indeed striking that neither the document on "The Future of Privacy" nor the 2010-2011 program of the EU Working Party art. 29 mention the directive 2003/98/EC. This set of rules subordinates the processing and re-use of the public sector information (PSI) to the provisions of D-95/46/EC on the protection of personal data [see art. 1 (4) of the PSI directive in the next section].

Eventually, there are some reasons explaining this otherwise puzzling silence.
On the one hand, notwithstanding the potential of PSI [Aichholzer & Burkert, 2004; Hugenholtz & Guibault, 2006], many EU Member States have inappropriately implemented the directive. It suffices to recall that the European Commission has taken five Member States – *i.e.*, Austria, Belgium, Portugal, Spain and Luxembourg – to the European Court of Justice for failing to implement the directive and, on March 19th, 2009, the Commission filed another infringement procedure against Italy.
On the other hand, even where Member States have started to exploit the potential of both PSI and the PSI directive, most of the data present little or no reference with people's personal data. So far, we are mostly talking about the re-use of, say, geographic information, army maps, land register and meteorological data, museums and local archives metadata, etc.
However, we need no prophetic powers in order to foresee that further implementation of the PSI directive will necessarily imply a number of privacy issues. Whereas the goal of the directive is to remove some of the barriers that are limiting the re-use of PSI, it is likely that the creation of added-value services with macro-economic relevance, like American PSI provides to the U.S. today, will run into the EU provisions on data protection.
This is precisely what both the Agencias de Protección de datos in Madrid and Barcelona stressed with their "Recommendations" from 2008. By paying attention to the possible re-use and processing of such data like civil service repositories, electoral data, universities' databanks, and the like, these Agencies insist on the necessity of adopting security measures and special regimes, along with the condition for habeas data guarantees like access, rectification, erasure, and blocking.
Moreover, the aforementioned Opinion on the concepts of "controller" and "processor" that the WP29 delivered on February 16th, 2010, is an important document, not centered on PSI and, yet, very interesting for our purposes. By examining cases of multiple controllers and processors in order to allocate responsibility in the legal system, the Opinion introduces some possible scenarios of interaction between D-2003/98/EC and D-95/46/EC.
Nonetheless, both the Recommendations and the WP29's Opinion fall short in coping with the risk that today's Information Society refrains from PSI re-use because of liabilities deriving from personal data protection. In order to illustrate this, let us examine the Spanish Recommendations from Madrid and Barcelona (section 4.1).
Then, we discuss the WP29's Opinion from 2010 (see below 4.2).
Finally, we introduce the "new principle" of *PSI by design* (section 4.3).

4.1 Spanish recommendations

A merit of the 2008 Spanish recommendations consists in having shed light on the relation between data protection norms and PSI re-use rules pursuant to art. 1 (4) of this latter directive, *i.e.*, D-2003/98/EC, which "leaves intact and in no way affects the level of protection of individuals with regard to the processing of personal data under the provisions of Community and national law, and in particular [it] does not alter the obligations and rights set out in Directive 95/46/EC."
According to the Agencia in Madrid, when processing and re-using PSI data, data controllers should follow some basic principles on the treatment of personal data. As stressed by the Recomendación 2/2008 from April 25th, such data should be "indispensable" and "minimized," so that the default rule provides for making such data anonymous most of the time, erased as soon as possible and, in any event, kept no longer than six months. Besides, the Agencia envisages additional specific regulations for both electoral and administrative data, in accordance with the architecture of that comprehensive legal framework later sponsored by the EU WPs's document on "The Future of Privacy" (see above 2.1).
In its recommendation 1/2008 from April 15th, the Agencia in Barcelona points out eight general conditions for the transmission of information on the internet, namely, the legitimacy and proportionality of the information, the exactitude and updating of the information transmitted, the

time limits of the transmission and the periodic review of the web content, besides duties on information, security measures and conditions for habeas data guarantees such as the data subject's right to access, rectify, erase, and block her data. While the aim is "to provide guidelines for action with regard to the transmission of information containing personal data on Internet websites," the recommendation is specifically "addressed to all bodies, entities and authorities forming part of or attached to public institutions in Catalonia, the Autonomous Government, local authorities [and] universities," including "public or private organizations that, in accordance with any contract, agreement or legal disposition, manage public services or exercise public functions."
However, one of the main side effects of current technological changes is that both "Web 2.0 services and cloud computing are blurring the distinction between data controllers, processors and data subjects" (see above 2.4). This is relevant when determining the responsibility for compliance with data protection rules, according to the functional approach proposed by the EU WP29 on February 16th, 2010 (see again supra 2.4).
What is more, such a functional approach becomes all the more appropriate, once we grasp the range of opportunities offered by PSI. Indeed, "the creation or improvement of services resulting from the data elaboration or aggregation can be encouraged by making available decentralized choices identifying innovative ways to use PSI. (…) In these terms PSI could be perceived as a platform, of which applications are still to be identified and written, just as the Internet or the Apple's iPhone" [Ricolfi, 2010].
After the 2008 Recommendations of the Spanish agencies, let us have a closer look at this new scenario.

4.2 Processors and controllers

In the aforementioned Opinion on the concepts of data processor and data controller, the WP29 insists on the necessity to adopt a functional approach in order to allocate responsibility in accordance with a substantial (rather than a formal) analysis. The WP29 proposes twenty six different examples so as to clarify its view. Here it suffices to mention example 11 of the Opinion, that is, the case of e-government portals, and example 15 on platforms for managing health data.

4.2.1 The case of e-government portals

The WP's example of e-government portals is particularly interesting because PSI can be re-used both "for improving public choices (e-governance)" and "for permitting citizens to take part in the public choices in a more sophisticated way (e-democracy)" [Ricolfi, 2010].
In a nutshell, the portal acts as an intermediary between citizens and the public administration units: While the portal transfers people's requests, it also deposits the public documents until they are re-used by the citizens. Besides the responsibility of each public administration unit, which remains controller of the data processed for its own purposes, can the portal be considered data controller in this case?
According to the EU WP29, it can.
Actually, the portal should be considered as a data controller because it processes data for further purposes than those for which the data was initially processed by each public administration unit. In order to facilitate e-government services, the portal collects the requests of citizens so as to transfer them to the competent public administration unit. Besides, the portal stores the public documents so as to regulate any access to them, *e.g.*, citizens' downloading of the documents.
The result is that, among other obligations, these portals ought to ensure the security of the system when transferring personal data from the user to the system of the public administration. At the macro-level, the EU WP29 claims that such a transfer is an "essential part of the set of processing operations carried out through the portal." As an intermediary between citizens and public

administration units, the portal is thus held responsible for the design of the system and how the latter processes people's personal data.

4.2.2 Platforms for managing health data

The second example concerns the hypothesis of a public authority which "establishes a national switch point regulating the exchange of patient data between healthcare providers."
Paradoxically, the number of data controllers involved, namely, all of the healthcare providers, may create an "unclear situation": It is not trivial to determine whom the patients have to address in order to exercise their rights, *e.g.*, make complaints, ask questions, and send requests for information, corrections or access personal data. Since "it can be argued that joint and several liability for all parties involved should be considered as a means of eliminating uncertainties," the WP suggests an autonomous responsibility for the public authority establishing the switch point.
At the end of the day, the public authority should be thought of both as a joint controller and as a point of contact for all of the patients' requests: This means that the public authority should be held responsible for the design of the platform and, therefore, indirectly, for how patients' data is used and processed.
This latter responsibility brings us back to the risk that public authorities may refrain from PSI re-use due to the cumbersome responsibilities deriving from personal data protection. It would not be the first time privacy is evoked so as to protect inertia or, even worse, to "conceal some sort of fraud" [Posner, 1983].

4.3 PSI by design

A "new principle" in the phrasing of the EU WPs's document, "Privacy by Design" is the subject of a number of works mainly focusing on data protection issues involved in the design of IC technologies [Abou-Tair and Berlik, 2006; Mitre *et al.*, 2006; Lioukadis *et al.*, 2007]. As Herbert A. Simon pointed out in his seminal book on *The Sciences of Artificial*, "in substantial part, design theory is aimed at broadening the capabilities of computers to aid design, drawing upon the tools of artificial intelligence and operations research" [Simon, 1996]. While scholars increasingly stress the specific impact of design or "architecture" and "code" on legal systems [Lessig, 1999; Katyal, 2002¸ 2003; Zittrain, 2008], it is interesting to further understand how artificial intelligence and operations research may aid design and, in doing so, impact on the structure and evolution of legal systems [Pagallo, 2007].
A mention should be made of an ongoing project on the "Neurona Ontology" developed by Pompeu Casanovas and his research team in Barcelona [Casellas *et al*., forthcoming]. The overall idea is to assume "ontologies" as the key form to implement new technological advances in the fields of both managing personal data and providing organizations and citizens "with better guarantees of proper access, storage, management and sharing of files." The explicit goal of the project is to help company officers and citizens "who may have little or no legal knowledge whatsoever."
Legal ontologies aim to represent knowledge through the modelling of concepts traditionally employed by lawyers, by formalizing norms, rights, or duties, in criminal law, administrative law, etc., in such a way that even a machine can comprehend and process this very information. We can further distinguish between the ontology containing all the relevant concepts of the problem domain through the use of taxonomies, and the ontology including rules and constraints that belong to a given problem domain [Breuker *et al.*, 2008]. An expert system should allow us to re-use PSI data in compliance with regulatory frameworks in data protection, as with e-government portals or healthcare switch points, via the conceptualization of classes, relations, properties, and instances of the problem domain.
Still, it could be argued that data protection regulations do not only include "top normative concepts" like validity, obligation, prohibition, and the like. These rules present highly context-

dependent normative concepts such as notions of personal data, security measures, or data controllers. These notions raise a number of relevant questions when reducing the informational complexity of a legal system in which concepts and relations are subject to evolution [Pagallo, 2007, 2010]. After all, we have analyzed some hermeneutical issues on data protection law, *e.g.*, matters of jurisdiction and sound definitions of equipment, which can be hardly reduced to an automation process. In the phrasing of Karen Yeung, "a rich body of scholarship concerning the theory and practice of 'traditional' rule-based regulation bears witness to the impossibility of designing regulatory standards in the form of legal rules that will hit their target with perfect accuracy" [Yeung, 2007].

Such technical difficulties in achieving the "perfect enforcement" of the law [Zittrain, 2007], illustrate why several projects concerning legal ontologies have adopted a bottom-up rather than a top-down approach, that is, "starting from smaller parts and sub-solutions to end up with global" answers [Casellas *et al.*, forthcoming]. While splitting the work into several tasks and assigning each to a working team, the evaluation phase consists not only in testing the internal consistency of the project but, according to Simon's "generator test-cycle," it involves the decomposition of the complete design into functional components. By generating alternatives and testing them against a set of requirements and constraints, "the test guarantees that important indirect consequences will be noticed and weighed. Alternative decompositions correspond to different ways of dividing the responsibilities for the final design between generators and tests" [Simon, 1996].

This ability to tackle our own ignorance helps us striking a balance between the know-how of legal ontologies and its limits. In a nutshell, the aim concerns privacy and PSI-reuse 'by' design, not 'as' design, *i.e.*, as if the goal were a sort of perfect self-enforcement technology which "collapses the public understanding of law with its application eliminating a useful interface between the law's terms and its application" [Zittrain, 2007]. What at stake, indeed, is the integration of compliance with regulatory frameworks through design policies, so that "privacy assurance must ideally become an organization's default mode of operation" [Cavoukian, 2009]. From the unfeasibility of automatizing all the mechanisms of data protection it does not follow the impossibility to restrict the discretion of company officers or public bureaucrats, while enhancing people's rights and encouraging behavioural change [Casanovas, 2009].

5. Conclusions

Along with "the future of" science, law and technology, the internet, the public domain, etc, scholars have often coped with "The Future of Privacy": For instance, this is precisely the subject matter of the last chapter of a comparative study on data protection published some years ago [Pagallo, 2008].

On that occasion, the forecast was summed up with the formula of "civic emergence" and the new ways in which we should grasp the interaction between private corporations and the public sector in the field of privacy law.

On one side, in spite of the threats to privacy created by the G. W. Bush's administration and its "war on terror," *e.g.*, the provisions of The Patriot Act, a reason of major concern involved databanks owned by private corporations. This was the case of the Canadian Internet Policy and Public Interest Clinic (CIPPIC)'s complaint against Facebook in May 2008, besides Facebook's own "terms-of-service"-crisis from February 2009 & May 2010, and the letter sent to Google's chief executive officer, Eric Schmidt, on April 19th, 2010. In the letter, the Privacy Commissioner of Canada, Jennifer Stoddart, and the heads of the data protection authorities of France, Germany, Israel, Italy, Ireland, Netherlands, New Zealand, Spain, and the United Kingdom, expressed their fears about privacy issues related to the new services of Google Buzz: "We therefore call on you, like all organizations entrusted with people's personal information, to incorporate fundamental privacy principles directly into the design of new online services."

On the other side, notwithstanding PET techniques, *e.g.*, encryption, it is all about the risks behind the use of commercial data, processed by private companies, in the name of alleged public interests. Starting with the Hadopi law passed by the French Parliament on October 22nd, 2009, it suffices to recall the "three strikes"-doctrine, that is, the law according to which internet users ought to be logged off after three notices of copyright infringement. The risk is that "feeling of permanent control" stressed by the German constitutional court in its judgment on data retention from March 2nd, 2010 [1 BvR 256/08].

Hence, some years after that 2008 forecast, how are the stars aligning today?

We propose to single out three aspects of the question.

First, it is likely we need to empower the data subjects over the next years as we define the responsibility of data controllers and strengthen the role of the public authorities in data protection: Will it prevail the open approach of EU WP29's Opinions or the more prudent ECJ jurisprudence?

Secondly, we need to mention some of the open issues that the WPs did not address in their document, *e.g.*, the new frontiers of biometrics and the relation between norms of PSI re-use and data protection provisions. It should be expected that also these subjects will contribute to work out that comprehensive legal framework required by the same European authorities.

Thirdly, we have matters of jurisdiction which the EU WPs have been debating over the last decade and that, nevertheless, are still far from finding a common, worldwide solution. Significantly, in the document on "The Future of Privacy," we are reminded that "the WP29 is writing an opinion on the concept of applicable law. The WP29 envisages advising the European Commission on this topic in the course of the upcoming year."

Yet, a final topic deserves our attention, namely, the "new principle" of privacy by design. By embedding data protection safeguards in IC technologies, the principle may represent a turning point in how we tackle most of the challenges mentioned above. Privacy by design could indeed help us strengthen people's habeas data and allow us to prevent the risk of hampering economic growth due to alleged privacy reasons. Moreover, privacy by design can represent an effective way to solve some of the extra-territorial legal effects and jurisdictional issues created by digital technology, in that privacy assurance can become a default mode of operation both for private companies and public institutions.

So, here comes our last conjecture: If it is not guaranteed that privacy by design will offer the one-size-fits-all solution to the problems we will be concerned with in the realm of data protection, privacy by design will be the key to understand how we have coped with today's privacy issues. It is not only a matter of technology, after all.

References

Abou-Tair, D. and Berlik, S. (2006), An ontology-based approach for managing and maintaining privacy in information systems, Lectures notes in computer science, Springer, 4275: 983-994

Aichholzer, G. and Burkert, H. (2004), Public sector information in the digital age. Between markets, public management and citizen's right, Elgar Publishing

Bauböck, R. (1994), Transnational citizenship: membership and rights in international migration, Elgar Publishing

Breuker, J., Casanovas, P., Klein, M.C.A., Francesconi E. (eds.) (2008), Law, ontologies and the semantic web: channelling the legal information flood, IOS Press

Brockman, M. (ed.) (2009), What's next? Dispatches on the future of science, Vintage

Brockman, M. (ed.) (2010), This will change everything. Ideas that will shape the world, Harper

Bynum, T. W. (2009), Philosophy and the information revolution, CEPE 2009: Eighth International Conference of Computer Ethics: Philosophical Enquiry, 26-28 June 2009, Ionian Academy Corfu, Greece

Casanovas, P. (2009), The future of law: relational justice and next generation of web service. In Fernandez-Barrera *et al.* (Eds.) (2009), Law and technology: looking into the future, European Press Academic Publishing, 137-156
Casellas, N., Torralba, S., Nieto, J.-E., Meroño, A., Roig, A., Reyes, M. and Casanovas, P. (forthcoming), The neurona ontology: a data protection compliance ontology
Cavoukian, A. (2009), Privacy by design, IPC Publications
Fernandez-Barrera, M., Nuno Gomes de Andrade, N, de Filippi, P., Viola de Azevedo Cunha, M., Sartor, G., and Casanovas, P. (eds.) (2009), Law and technology: looking into the future, European Press Academic Publishing
Ford, K. W. (2010), Reading minds, in Brockman, M. (ed.), This will change everything, Harper, 141-142
Garrett Lisi, A. (2010), Changes in the changers, in Brockman, M. (ed.), This will change everything, Harper, 270-273
Goldsmith, J. (1998), Against cyberanarchy, University of Chicago Law Review, 65: 1199-1250
Holtzman, D. H. (2006), Privacy lost. How technology is endangering your privacy, Jossey-Bass
Horner, D. S. (2010), Metaphors in orbit: revolution, logical malleability, generativity and the future of the internet, ETHICOMP 2010: The "backwards, forwards and sideways" changes of ICT, edited by M. Arias-Oliva, T. W. Bynum, S. Rogerson e T. Torres-Corona, Universitat Rovira I Virgili, Tarragona, Spain, 301-308
Hugenholtz, B. and Guibaault, L. (eds.) (2006), The future of the public domain. Identifying the commons in information law, Kluwer
Jarfinkel, S. (2000), Database nation. The death of privacy in the 21st century, O'Reilly
Jessup, P. C. (1956), Transnational law, Yale University Press
Katyal, N. (2002), Architecture as crime control, Yale Law Journal, 111: 1039-1139
Katyal, N. (2003), Digital architecture as crime control, Yale Law Journal, 112: 101-129
Kuner, Ch. (2003), European data privacy law and online business, Oxford University Press
Lioukadis, G., Lioudakisa, G., Koutsoloukasa, E., Tselikasa, N., Kapellakia, S., Prezerakosa, G., Kaklamania, D. and Venierisa, I. (2007), A middleware architecture for privacy protection, The International Journal of Computer and Telecommunications Networking, 51(16): 4679-4696
Lessig., L. (1999), Code and other laws of cyberspace, Basic Books
Lessig, L. (2002), Privacy as property, Social Research, 69: 247-269
Mitre, H., González-Tablas, A., Ramos, B., and Ribagorda, A. (2006), A legal ontology to support privacy preservation in location-based services, Lecture notes in computer science, Springer, 4278: 1755-1764
Pagallo, U. (2007), "Small world" paradigm and empirical research in legal ontologies: a topological approach, The multilanguage complexity of European law: methodologies in comparison, edited by G. Ajani, G. Peruginelli, G. Sartor, D. Tiscornia European Press Academic Publishing, 195-210
Pagallo, U. (2008), La tutela della privacy negli Stati Uniti d'America e in Europa: modelli giuridici a confronto, Giuffrè
Pagallo, U. (2009), Sul principio di responsabilità giuridica in rete, Il diritto dell'informazione e dell'informatica, XXV(4-5): 705-734
Pagallo, U. (2010), As law goes by: topology, ontology, evolution. AICOL 2009, edited by P. Casanovas, U. Pagallo, G. Sartor, G. Ajani, Springer
Posner, R. A. (1983), Privacy and related interests, The Economics of justice, Harvard University Press, 299-347
Post, D. G. (2002), Against "against cyberanarchy", Berkeley Technological Law Journal, 17: 1365-1383
Ricolfi, M. (2010), Public sector information: a general overview, Extracting value from PSI: legal framework and regional policies, EVPSI meeting at the University of Turin, Italy, on March 26th

Sartor, G., Viola de Azevedo Cunha, M. (2010), The Italian google-case: privacy, freedom of speech and responsibility of providers for user-generated contents (May 11, 2010). Available at SSRN: http://ssrn.com/abstract=1604411
Simon, H. A. (1996), The sciences of the artificial, The MIT Press
Strickling, L. E. (2010), The internet: evolving responsibility for preserving a first amendment miracle, The Media Institute, February 24th, 2010
Sykes, C. (1999), The end of privacy. The attack on personal rights at home, at work, on-line, and in court, St. Martin's Griffin
Tavani, H. T. (2007), Philosophical theories of privacy: implications for an adequate online privacy policy, Metaphilosophy, 38(1): 1-22
Volkman, R. (2003), Privacy as life, liberty, property, Ethics and Information Technology, 5(4): 199-210
Yeung, K. (2007), Towards an understanding of regulation by design, Regulating technologies: legal futures, regulatory frames and technological fixes, edited by R. Brownsword, K. Yeung, Hart Publishing, 79-108
Zittrain, J. (2007), Perfect enforcement on tomorrow's internet, Regulating technologies: legal futures, regulatory frames and technological fixes, edited by R. Brownsword, K. Yeung, Hart Publishing, 125-156
Zittrain, J. (2008), The future of the internet and how to stop it, Yale University Press
Zumbansen, P. (2006), Transnational law, Encyclopedia of Comparative Law, Elgar, 738-754