Yale Journal of Law and Technology

Volume 15
Issue 1 *Yale Journal of Law and Technology*

Article 3

2013

Reverse Engineering Informational Privacy Law

Michael Birnhack
Yale Law School

REVERSE ENGINEERING INFORMATIONAL PRIVACY LAW

Michael Birnhack*

15 YALE J.L. & TECH. 24 (2012)

ABSTRACT

Is technology-neutral legislation possible? Technological neutrality in legislation is often praised for its flexibility and ability to apply to future technologies. Yet, time and again we realize that even if the law did not name any technology, it was nevertheless based on an image of a particular technology. When new technologies appear, they expose the underlying technological mindset of the existing law. This article suggests that we read technology-related laws to uncover their hidden technological mindset so that we can better understand the law and prepare for the future. Reverse engineering the law is an interpretive mode, tailored to uncover the technological layer of the law.

After locating the discussion within the emerging research paradigm of law and technology, the article unpacks the meaning of technology-neutral legislation and points to three possible justifications thereof: flexibility, innovation and harmonization. The article then suggests an initial typology of the range of legislative choices, one that is richer than a binary all-or-nothing choice. The typology is based on three continuums: means-end, promotion-restriction and abstract-concrete. The three continuums can assist policy makers in deciding whether to attempt legislating in a technologically neutral matter or not. The article then explains the methodology of reverse engineering the law.

The next step is to challenge the claim of neutrality in the context of informational privacy. Proposals to amend the law are on the tables of policy-makers in the United States and in the European Union (EU). I focus on the current global engine of data protection law, the 1995 EU Data Protection Directive. The reverse engineering of the Directive indicates that it is more technology-neutral than we might have expected from an

---

* Professor of Law, Faculty of Law, Tel Aviv University. I thank Julie Cohen, Stewart Dresner, Talia Fisher, Paul Ohm, Haim Wismonsky, Tal Zarsky, participants at the 39th Telecommunications Policy Research Conference (Washington, Sep. 2011) and my colleagues at the PRACTIS research project, for helpful comments; and the Institute of Advanced Legal Studies (IALS), University of London, where I was an Associate Fellow while researching this article. Thanks are due also to the attentive editors of the Yale Journal of Law and Technology for the helpful comments.

instrument that was composed in the early 1990s based on laws from the early 1970s. Nevertheless, a close reading reveals the Directive's underlying technological mindset and hidden assumptions. I conclude that pure technologically neutral legislation is, to a great extent, a myth.

15 YALE J.L. & TECH. 24 (2012) 2012-2013

TABLE OF CONTENTS

INTRODUCTION 27
I. FRAMEWORK: LAW AND TECHNOLOGY 32
II. LEGISLATIVE TECHNIQUES FOR A DIGITAL ENVIRONMENT.....35
A. Technology-Neutral Legislation 36
B. Considerations and Justifications..... 38
1. Flexibility.....38
2. Innovation.....42
3. Harmonization.....44
C. An Initial Typology 45
1. What does the law regulate? Ends—Means.....45
2. How does the law treat technology? Promotion—Restriction.....48
3. How does the law define the regulated technology? Abstract—Concrete.....49
4. Who regulates technology?.....51
D. Interim Summary..... 51
III. REVERSE ENGINEERING THE LAW.....52
IV. INFORMATIONAL PRIVACY.....56
A. United States: Privacy and Private Information 57
B. The OECD and Data Protection in Europe..... 59
1. International Initiatives 59
2. Enter the European Union.....61
3. The EU Directive: The Law Follows Personal Data...63
4. New Initiatives and Proposals 66
V. REVERSE ENGINEERING THE DATA PROTECTION DIRECTIVE....68
A. The Directive and Technology..... 69
B. The Directive and Technology Neutrality..... 73
1. Personal Data.....74
2. Processing of Personal Data 77
3. Personal Data Filing System – aka Database.....87
CONCLUSION.....89

INTRODUCTION

This article explores a paradox about technology-related legislation. On the one hand, legislators often declare that their motivation in enacting a new law is driven by the implications of new technologies. Indeed, laws do not regulate technology *tabula rasa*. When the law enters a technological field, it necessarily carries with it an image of the technology it is about to address. This technological image might be explicit or hidden; it might be based on a factual inquiry or on a general perception; it might be accurate or misguided. The underlying image shapes the law's mindset regarding its technological subject matter.

On the other hand, a common claim about technology-related laws is that they are technology-neutral; namely, that they can apply to all relevant technologies. Legislative technological neutrality is said to achieve several important goals, which I shall identify as flexibility, innovation, and harmonization. These three goals, if achieved, could assure that the law remains relevant even in light of newer technologies that were not anticipated at the time of legislation (*flexibility*); they promote the development of new and hopefully better technologies—or at least they do not hinder it (*innovation*); and they can smooth and streamline the diffusion of technologies (*harmonization*). Technological neutrality also attempts to overcome any technological bias that the law might have. In other words, technology-neutral laws purport to regulate technology without envisaging an image of the regulated technology. Hence the paradox: can the law regulate technology and yet remain blind as to the regulated technology? Is technology-neutral legislation possible?

This article suggests that we read technology-related laws so as to uncover their technological mindset. This is the *reverse engineering of the law*. Such a reading is an interpretive tool that can assist us in evaluating the law and the legal ramifications of new technologies. The proposed reading—the reverse engineering of the law—is different from a lawyer's legal reading of the law, which aims to figure out the scope of a given law ("What is the law?"). It differs from an interpretative mode that searches for a law's purpose ("What is the law meant to achieve?"). Nor is it a historical reading, aimed at figuring out the original intention of its legislators ("What did the legislators intend?"). Instead, the proposed reading is interested in the legislation's attitude as to technology: "What is the law's underlying technological mindset?" I seek the legislation's meaning in its outcome, rather than in the intentions of the law's drafters or the legislative history. This reading is informed by literary criticism in its focus on the text and

the subtext. Like other interpretive modes, it tries to expose hidden assumptions.

One possible explanation of the paradox would be to deny the first claim, that the law has an underlying image about the regulated technology. However, this answer would be too cursory. Time and again we realize that a law that seemed to be technology-neutral at one point (usually the time of its legislation), is in fact based on a particular technology, albeit in a general manner. We often realize the technological mindset that is embedded in the law only once a new technological paradigm replaces the previous one. This was true of copyright law when the digital environment challenged analogue works of authorship, it was true of various laws that require a particular form for contracts (such as "writing" or a "signature") and it is true once again in the realm of privacy law. New technologies expose how the current law was shaped around a particular vision of technology, snapshotted in its past social context, even if a seemingly neutral language was applied.

Accordingly, I suggest that we read the law as a socio-cultural text that consists of several layers of meanings. Underneath the plain text and the legal rules, there are hidden layers, composed of the legislature's assumptions as to society, culture, technology, and probably much more. Here, I focus on deciphering the technological layer by reverse engineering the law so as to expose its technological mindset. The case study applied here is informational privacy law - more specifically, the EU Data Protection Directive.[1]

The law of informational privacy is about to change. There are continuous demands for a new approach to this legal field. The triggers are new technologies, globalization, new business models, and national security interests, each pulling in a different direction. My focus here is on the impact of new technologies. Following several high profile *privacy events* that were met with public dismay and popular resistance, there has been a bottom-up demand directed at politicians "to do something." Some recent privacy events include the revelation that Google, in its Street View project, collected not only photographs of houses (and people and cars), but also data sent over open WiFi networks;[2] the revelation that Apple's iPhone and iPad stored the geographical position of

[1] Directive 95/46, of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) (EC) [hereinafter Council Directive 95/46].

[2] Google admitted its mistake on its official blog. *WiFi data collection: An update,* GOOGLE BLOG (May 14, 2010), http://googleblog.blogspot.com/2010/05/wifi-data-collection-update.html.

the devices in a hidden folder,[3] and several events in which Facebook used its users' personal data in ways that the latter disagreed with, at least once they learned about it.[4]

The popular bottom-up demands join political factors that push towards new regulatory approaches to privacy. In the United States, the Federal Trade Commission (FTC) published a Preliminary Staff Report in late 2010 and a final report in March 2012 suggesting a normative framework for businesses regarding the commercial use of consumer data.[5] In Europe, there are on-going discussions about a substantial amendment to the legal framework of data protection—the European term for informational privacy. In early 2012, the European Commission published a proposal for a new legal regime in the form of a European Regulation.[6] Elsewhere, governments and legislatures are busy examining similar issues. One interesting suggestion that has gained much interest and attention in professional circles is Privacy by Design (PbD), promoted by Ontario's Information

[3] The discovery was made by Alasdair Allan and Pete Warden at the Where 2.0 Conference. Alasdair Allan & Pete Warden, *Got an iPhone or 3G iPad? Apple is recording your moves*, O'REILLY RADAR (Apr. 20, 2011), http://radar.oreilly.com/2011/04/apple-location-tracking.html.

[4] *See*, *e.g.*, the Beacon feature that Facebook launched in 2007; the friends of a Facebook user were informed of the user's actions taken on affiliated websites. A lawsuit followed and was settled. *See* Findings of Fact, Conclusions of Law, and Order Approving Settlement, Lane v. Facebook, Inc., No. C 08-3845 RS (N.D. Cal. May 24, 2010), *available at* http://www.scribd.com/doc/28530843/Lane-v-Facebook-N-D-Cal-Order-Approving-Settlement. Another Facebook privacy event was the automatic tagging of user's photos, without their prior consent. *See Facebook 'Face Recognition' Feature Draws Privacy Scrutiny*, N.Y. TIMES (June 9, 2011), http://www.nytimes.com/2011/06/09/technology/09facebook.html.

[5] FTC STAFF REPORT, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE – A PROPOSED FRAMEWORK FOR BUSINESS AND POLICYMAKERS (2010); FTC REPORT, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE – RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS (2012). The report suggests that (1) Companies should adopt a "privacy by design" approach; (2) Companies should provide simplified choices for businesses and consumers; and (3) Companies should make their data practices more transparent. The Final Report retained the general framework proposed by the Preliminary Report, but narrowed its scope and its demand for universal consumer choice and emphasized the need to regulate information brokers.

[6] *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 (Jan. 25, 2012), *available at* http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf [hereinafter *Proposed GDP Regulation*]. A Regulation is directly applicable within the 27 Member States that comprise the European Union.

Commissioner, Anne Cavoukian.[7] The idea is simple, though not easy to apply: plan and design technology so it takes care of privacy concerns to begin with rather than try and fix them later, once it is difficult, expensive, and in many cases, too late.[8] PbD tries to inject legal notions of privacy into the technology in an explicit manner: it is a legal attempt to shape technology. Here, I wish to explore the other direction: how the technology shaped the law.

The article wishes to make three contributions, from the abstract to the concrete: first, to elaborate on our understanding of the relationship between law and technology; second, to suggest the interpretive methodology of reverse engineering the law; and third, to expose the hidden technological assumptions of informational privacy law. Once we realize what the current law's technological assumptions are, we can better understand the law in a coherent way. This is an interpretive advantage. Moreover, once we uncover the law's technological mindset, we are better equipped to address new technologies. We might not yet know how to regulate them, if at all, but at least we know the limits of our current legal scheme. This is a legislative advantage: reverse engineering the law can provide a better roadmap for prospective legislation.[9]

Part I locates the project within the still relatively new academic paradigm of law and technology. I discuss the dialectical relationship between law and technology in which they converse and respond to each other, rather than engage in an outright battle or a disconnection. Part II turns to the other prong of the above mentioned paradox: technology-neutral legislation. It unpacks the much-asserted call for technology-neutral legislation rather than technology-specific legislation. I point to three main considerations that may justify the neutrality position: flexibility, innovation and harmonization. I then offer an initial typology of technology-

---

[7] *See* Ann Cavoukian, *Privacy by Design: The 7 Foundational Principles*, PRIVACY BY DESIGN, http://privacybydesign.ca (last visited Jan. 9, 2013). For an analysis, see Ira S. Rubinstein, *Regulating Privacy by Design*, 26 BERKELEY TECH. L.J. 1409 (2011).

[8] *See*, *e.g.*, Ken Anderson & Michelle Chibba, *Privacy by Design: Meeting the Privacy Challenge in a Changing World*, *in* PATENTS, COPYRIGHTS, TRADEMARKS, AND LITERARY PROPERTY (2011).

[9] The next step, not carried out here, would be to compare the exposed underlying technological assumptions of the law to the traits of emerging—and more so—future technologies. Such an analysis is conducted under the auspice of PRACTIS, a European research group, focusing on the privacy implications of future technologies. *See Description of Work*, PRACTIS - PRIVACY APPRAISING CHALLENGES TO TECHNOLOGIES AND ETHICS, www.practis.org (last visited Jan. 9, 2012).

neutral legislation and point out its limits. Part III introduces and explains the methodology of reverse engineering the law. Part IV turns to the case study discussed here and outlines the legal regime of informational privacy. I provide a condensed overview of the different legal approaches to privacy interests in personal data, especially the American sectoral approach and the European omnibus approach. Both legal regimes, to the extent that they address the matter, build substantially on the notion of Fair Information Principles (FIPs). The European Directive on Data Protection of 1995 (95/46/EC) has been the engine of this emerging global regime. Due to its global influence, it is today the most important data protection instrument and hence serves as the leading case study.[10]

Part V turns to reading the European Directive so as to reverse engineer it. I focus on its key constructs. This reading indicates that data protection law as exemplified in the Directive is more technological-neutral than we might have expected from an instrument that was composed in the early 1990s based on laws from the early 1970s and guidelines from the early 1980s. Nevertheless, the close reading reveals some of its underlying technological mindset and assumptions.

First, I will argue that current informational privacy law assumes a linear sequence as to personal data, in which the data is first collected and stored, then used in various ways and then transferred to another controller for further use. This linear view assumes that each segment can be placed under the responsibility of a relevant player. The linear view enables us to see that there are very few meeting points between the data subject (i.e., the individuals) and the data controller (i.e., the collector and processor of the data), which can serve as points of control where data subjects can exercise their rights. Second, the legal regime of data protection has a strong focus on the notion of a database. The idea that the data is stored in some giant database seems to have carried a great influence on the drafters of the Directive, or at least the outcome indicates so.

At the end of the day, the answer to the paradox is that the law is less technologically neutral than we currently admit. Drafting legislation in a technology-neutral manner might be a worthy goal, but we should acknowledge that success in achieving

[10] *See* Michael D. Birnhack, *The EU Data Protection Directive: An Engine of a Global Regime*, 24 COMP. L. & SEC. REP. 508 (2008); Christopher Kuner, *An International Legal Framework for Data Protection: Issues and Prospects*, 25 COMP. L. & SEC. REP. 307 (2009). A few American scholars referred to the Directive as aggressive. I find it far less aggressive than these statements. *See* Birnhack, *supra*.

this goal can, at best, be partial. To a large extent, technology-neutral legislation is a myth.

I. FRAMEWORK: LAW AND TECHNOLOGY

This Part lays the theoretical framework for the reverse engineering of data protection law. I locate the issue of informational privacy within the broader discussion of the relationship between law and technology.

The digital revolution created both new opportunities and new risks. The latter, more than the former, triggered the law. Time and again we realize that we need to quickly figure out whether old laws apply to the new environment and, if so, how. If the old laws do not fit the new situation, we have to decide whether to enact new laws. By now, these are familiar discussions: should we regulate online speech so as to protect our children from exposure to harmful content?[11] What is the proper balance between copyright owners and users online?[12] Are ISPs and other intermediaries liable for harmful acts done by end-users?[13] Should anonymous users be unmasked?[14] The list of questions is endless. Each deserved much attention by legislatures, courts, scholars and the public at large. The debates gave rise to a meta-discussion: Is technology regulable at all? Should the law do so? The scholarship about the relationship between the law and technology, especially information technology, covers these questions.

I summarize this debate in broad-brush. My purpose is instrumental: to explore the more subtle interactions between law and technology. Once the legislature concludes that it has the power and that it is wise to intervene in some way to regulate the activity that takes place within a technological environment or perhaps even regulate technology directly, the legislators proceed with a certain perception of the regulated subject matter. This is what I call the *technological mindset*.

---

[11] *See*, *e.g.*, Symposium, *Do Children Have the Same First Amendment Rights as Adults?* 79 CHI.-KENT L. REV. 3 (2004).

[12] *See*, *e.g.*, JAMES BOYLE, THE PUBLIC DOMAIN: ENCLOSING THE COMMONS OF THE MIND (2010).

[13] *Compare* 47 U.S.C. § 230 (2006) (providing ISPs with broad immunity from liability for various users' torts), *with* 17 U.S.C. § 512 (2006) (providing ISPs with limited liability, based upon some conditions, from liability under copyright law).

[14] The law on this point is unsettled and different state courts in the United States articulated various legal tests on the matter. See, for example, Pilchesky v. Gatelli, 12 A.3d 430 (Pa. Super. Ct. 2011), and a discussion of the various tests in Nathaniel Gleicher, Note, *John Doe Subpoenas: Toward a Consistent Legal Standard*, 118 YALE L.J. 320 (2008).

One view of the law and technology debate considers technology to be a unique phenomenon, which is by its nature unregulable. Call it a *technology-separatist view*. In its extreme version, the argument is that technology develops according to its own rules, in a separate world, apart from that of other social phenomena, especially the law. According to this view, the law cannot interfere with the course of technology, which is taken to be pre-determined. Any attempt to interfere is useless and a waste of time and effort on behalf of the lawyers. It could also be an unnecessary disruption that could damage the inevitable process, at least until technology defies the law. Kevin Kelly's assertion of "what technology wants" reflects this approach. Kelly assumes that technology has an internal, independent drive.[15] The deterministic view isolates technology from society and subjects the latter to the former.[16]

Somewhat milder views argue that the law should not interfere in the development of the technology and leave it to its own devices. John Perry Barlow's oft-quoted 1996 Declaration of Independence of Cyberspace urged the "Governments of the Industrial World," the "weary giants of flesh and steel," to "leave us alone." Cyberspace, Barlow declared, "is an act of nature and it grows itself through our collective actions."[17] Barlow's declaration was based, so it seems, on a libertarian set of values. Another famous argument, by David Johnson and David Post also in 1996, was that cyberspace requires a distinct legal system.[18] Both these views do not exclude law entirely from the technological realm, but they do narrow the permitted intervention - to self-regulation in Barlow's case and to a *sui generis* internet law, in the case of Johnson and Post.

The other side of the debate challenges the basic assumptions of the deterministic view. Call it a *socio-technological view*. First, the socio-technological view emphasizes that technologies are not void of values. Each technology reflects a value or values (including conflicting values in some cases).[19] The deterministic, technology-separatist view might agree with this idea, but it would argue that the values are given and fixed, as they

---

[15] KEVIN KELLY, WHAT TECHNOLOGY WANTS (2010).

[16] For a critique of technological determinism, see EVGENY MOROZOV, THE NET DELUSION: THE DARK SIDE OF INTERNET FREEDOM 289-95 (2011).

[17] John Perry Barlow, *A Declaration of the Independence of Cyberspace*, ELECTRONIC FRONTIER FOUND. (Feb. 8, 1996), https://projects.eff.org/~barlow/Declaration-Final.html.

[18] David R. Johnson & David Post, *Law and Borders – The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367 (1996).

[19] *See*, *e.g.*, HUMAN VALUES AND THE DESIGN OF COMPUTER TECHNOLOGY (Batya Friedman ed., 1997); MOROZOV, *supra* note 16, at 295-99 (explaining why technology is never neutral.).

developed in the separate technological universe. With the separatist view, we are left, at most, with the choice of figuring out the embedded values and learning how to use such technologies. The socio-technological view, by contrast, is inclusive. It rejects the argument that the technology-embedded values are an unchangeable fact. Accordingly, we can actively design technologies to reflect values that we cherish. Moreover, technology and its embedded values are a social construct. Society, through various processes, decides what each technology means, how it is used, and ultimately, whether it is a "good" technology or a "bad" one.

A second element of the socio-technological view, which stems directly from the previous one, is that as a matter of principle, technology is subject to the law just like any other human activity. The law provides a discursive platform to debate the issues and enable society to make decisions about values and technologies. According to this view in its extreme form, there is nothing particularly unique in technology, at least not in the basic question of its regulability.[20] Under the socio-technological view, technology is a product of members of societies (individuals, corporations or governments) and there is no a-priori reason to exclude technology from the reach of the law. The question is no longer *if* it should be regulated, but rather *how* to regulate it.

Between the two extreme ends of the deterministic, separatist view and the socio-technological view, there are many possible points. Technology reacts and interacts with the law in many ways. Sometimes law and technology join together to achieve a common goal. For example, Privacy Enhancing Technologies (PETs) and privacy law both attempt to protect our privacy.[21] Sometimes law and technology compete with one another and constantly try to outreach one another. The application of copyright law to file-sharing systems illustrates this point. The law imposed its rules on systems such as Napster, a move which was met by a counter-action: new peer-to-peer (p2p) systems were designed which were less regulable.[22] Examples were Aimster (which encrypted users' file exchange) and Grokster (which purported to be a distributed network but in fact induced users to

[20] Indeed, as a matter of fact, governments around the world do regulate information technology, cyberspace included, or at least they try to do so. Johnson and Post's argument was thought-provoking at the time and drew the attention to many of these issues, but their suggestion has not yet materialized.

[21] On PETs, see Herbert Burkert, *Privacy-Enhancing Technologies: Typology, Critique, Vision*, *in* TECHNOLOGY AND PRIVACY: THE NEW LANDSCAPE 125 (Philip E. Agre & Marc Rotenberg eds., 2001).

[22] *See* A&M Records, Inc. v. Napster, Inc., 284 F.3d 1091 (9th Cir. 2002).

exchange copyrighted files).[23] The law responded once again, finding Aimster and Grokster to contribute to and induce copyright infringement, respectively.[24] Technology responded once again, with truly distributed systems.[25] The cat and mouse match is not over and probably will not be over in the near future.[26]

The possibility of regulating technology does not mean that we must take this course. When the choice to regulate technology is made, there is a rich arsenal of legal tools to do so: local regulation and international instruments, criminal and civil laws, providing positive and negative incentives, addressing one link in a chain of activity so as to curtail it,[27] and other legal tools.

Subjecting technology to regulation does not mean being dogmatic. Before deciding if and how to regulate, legislators should carefully study the technology and understand its embedded values. On the legal side, we need to be clear as to what our goals are in the specific context: which norms does the law strive to achieve? If there are conflicting interests, how should we prioritize or balance them? After figuring these substantive issues, we need to get into the details and choose the best legislative mechanism and technique. Importantly, this might also mean that in certain cases, we should refrain from regulating at all. This article proceeds within the socio-technological approach. It is located within a paradigm that views technology as a product of social activity, which has social implications rather than an isolated, external and untouchable entity.

II. LEGISLATIVE TECHNIQUES FOR A DIGITAL ENVIRONMENT

Once we acknowledge the complex, multi-faceted, and dialectical relationship between law and technology, we can look

[23] *See* In re Aimster Copyright Litigation, 334 F.3d 643, 646 (7th Cir. 2003); MGM, Inc. v. Grokster, Ltd., 545 U.S. 913 (2005).

[24] In re Aimster Copyright Litigation, 334 F.3d at 646; *Grokster*, 545 U.S. 913.

[25] The copyright owners in the music industry turned to prosecute the individual users in a series of multi-defendant litigation. *See, e.g.*, Capitol Records, Inc. v. Thomas-Rasset, 692 F.3d 899 (8th Cir. 2012).

[26] For the subsequent round, see Eldar Haber, *The French Revolution 2.0: Copyright and the Three Strikes Policy*, 2 HARV. J. SPORTS & ENT. L. 297 (2011) (discussing the industry-driven initiatives to disconnect allegedly repeat infringers from the Internet altogether). Further rounds were the successful public battle over the Stop Online Privacy Act (SOPA), H.R. 3261, 112th Cong. (2011) and Protect IP Act (PIPA), S. 968, 112th Cong. (2011), and on the international level, the controversial Anti-Counterfeiting Agreement (ACTA).

[27] For addressing various links in the chain of a regulated activity, see Michael D. Birnhack & Jacob H. Rowbottom, *Shielding Children: The European Way*, 79 CHI.-KENT L. REV. 175 (2004) (comparing European attempts to regulate online content which is deemed harmful to minors to American attempts).

closer at some of these nuances. One of the important yet often overlooked aspects is that of legislative technique: how to translate the goals and means into the law itself. A recurrent position advocates that the law is drafted in a technologically-neutral manner. This Part challenges this idea and questions its very possibility.

Section A sets the question; Section B provides an overview of the main considerations for and against the two possible legislative techniques: technological-neutral and technological-specific legislation; and Section C offers a brief typology of technology-neutral legislation along several parameters, suggesting that we replace a dichotomous approach with a series of continuums that form a complex legislative matrix. Finally, Section D provides an interim summary.

A. Technology-Neutral Legislation

Statements about the desirability of *technology-neutral* legislation abound.[28] The idea is simple: the law should not name, specify or describe a particular technology, but rather speak in broader terms that can encompass more than one technology and, hopefully, would cover future technologies that are not yet known

[28] For an example in copyright law, see the report of the Committee on Commerce, H.R. REP. NO. 105-551(II), at 25 (1998), on the Digital Millennium Copyright Act of 1998: "The Committee thus seeks to protect the interests of copyright owners in the digital environment, while ensuring that copyright law remain technology neutral"; and the discussion in Daniel Gervais, *The Tangled Web of UGC: Making Copyright Sense of User-Generated Content*, 11 VAND. J. ENT. & TECH. L. 841, 857 (2009).

In patent law see, for example, Ben McEniery, *Physicality and the Information Age: A Normative Perspective on the Patent Eligibility of Non-Physical Methods*, 10 CHI.-KENT J. INTELL. PROP. 106, 109 (2010), arguing that "a technology-neutral subject matter test is the appropriate standard in an age where new advances in information technology and information management are likely to become increasingly important in the economy in the 21st century."

In the context of electronic signatures, see, for example, Anjanette Raymond, *Improving Confidence in Cross Border Electronic Commerce: Communication, Signature, and Authentication Devices*, 14(11) J. INTERNET L. 25, 33 (2011): "At the cross border level the law must begin to be harmonized, which can only occur if the majority of domestic systems recognize the need for technology neutral drafting techniques."

In telecommunication law, see, for example, Ellen P. Goodman & Anne H. Chen, *Digital Public Service Media Networks to Advance Broadband and Enrich Connected Communities*, 9 J. TELECOMM. & HIGH TECH. L. 81, 119 (2011), advocating a new Public Service Media which maintains a technology-neutral position.

In environmental law, see for example, David E. Adelman & John H. Barton, *Environmental Regulation for Agriculture: Towards a Framework to Promote Sustainable Intensive Agriculture*, 21 STAN. ENVT'L. L.J. 3, 40 (2002), proposing technology-neutral regulations of agricultural inputs and emissions.

at the time of legislation. The guidance that the law should be neutral in this sense is a much heralded and cherished principle, though it is not always followed. Those who argue that *technology-specific* legislation is preferable often find themselves arguing against the stream.[29] Naturally, we find statements about the importance of the technology-neutral stance mostly in fields that have direct encounters with technology, such as intellectual property,[30] e-commerce,[31] telecommunications,[32] environmental law,[33] and, in recent years, privacy law.[34] However, a closer examination of these laws and their reference to technology indicates that their claims or aspirations for technology neutrality mean quite a few different things. Accordingly, we should unpack the concept of technology neutrality.

The choice between technology-neutral or technology-specific legislation has a familiar jurisprudential parallel, the distinction between standards and rules. The latter discussion is relevant for the law in general. H.L.A. Hart offered a now-classic jurisprudential example: a legal rule that prohibits vehicles in a park.[35] It seems to be a straightforward rule with a clear core, but it has an unclear penumbra. While Hart used the example to argue that the law is not as indeterminate as the legal realists have

---

[29] *See, e.g.*, Paul Ohm, *The Argument Against Technology-Neutral Surveillance Laws*, 88 TEX. L. REV. 1685 (2010) (favoring technology-specific legislation in surveillance law); Laura Hildner, Note, *Defusing the Threat of RFID: Protecting Consumer Privacy through Technology-Specific Legislation at the State Level*, 41 HARV. C.R.-C.L. L. REV. 133, 138 (2006) (arguing that "RFID technology poses a distinct and significant threat to consumer privacy even in a society where private entities routinely intrude upon individuals" and hence advocates technology-specific state legislation in addition to "baseline privacy legislation").

[30] *See* Gervais, *supra* note 28.

[31] *See, e.g.*, Michael A. Geist, *Is There a There There? Toward Greater Certainty for Internet Jurisdiction*, 16 BERKELEY TECH. L.J. 1345, 1359 (2001) (listing technology neutrality as one of four policy considerations in developing a test for internet jurisdiction and supporting neutrality due to its ability to withstand technological changes); Raymond, *supra* note 28 (discussing neutrality regarding electronic signatures).

[32] *See* Goodman & Chen, *Digital Public Service*, *supra* note 28; Ellen P. Goodman & Anne H. Chen, *Modeling Policy for New Public Service Media Networks*, 24 HARV. J.L. & TECH. 111, 123 n. 52 (2010) (noting the White House and the FCC's technological neutrality policy regarding the electromagnetic spectrum).

[33] *See, e.g.*, Adelman & Barton, *supra* note 28.

[34] *See infra* Part VI.

[35] *See* H.L.A. HART, THE CONCEPT OF LAW 125-26 (2d ed. 1994). Hart's example, first articulated in 1961, is still subject to debate. *See, e.g.*, Frederick Schauer, *A Critical Guide to Vehicles in the Park*, 83 N.Y.U. L. REV. 1109 (2008).

argued, the example illustrates that rules do have such an inherent indeterminate element. Importantly, technology plays a critical role in rendering the rule indeterminate. The advancement of new technologies enables us to add more examples to the no-vehicle-in-the-park prohibition: is an electric wheelchair a "vehicle?" What about a Segway? The debate that Hart referred to and that his example further provoked was mostly about interpretation. The debate discussed here, about technology-neutral/technology-specific legislation can be restated in these terms: technology-neutral laws are equivalent to standards and the technology-specific laws are equivalent to rules. The technological context draws our attention from the act of interpretation to the act of legislation.

B. Considerations and Justifications

Why does the legislative technique matter? Several considerations are relevant when assessing legislation and choosing either a technology-neutral approach or a technology-specific one. If the considerations apply, they become justifications for the chosen technique. I discuss three main considerations that favor the former and the responses on behalf of the latter: flexibility, innovation and harmonization.[36]

1. Flexibility

First and foremost, a technology-neutral legislative technique is flexible, in that it can cover a wide range of technologies. Given that the law cannot anticipate new

[36] *Cf.* Ohm, *supra* note 29. In the context of surveillance law, Ohm classified the considerations under different titles: (1) consistency, by which he means "the need to avoid arbitrary distinctions between technologies that should be treated alike." (*Id.* at 1691-92); (2) keeping up with technological change (*Id.* at 1692-94), pointing out that technology-specific laws tend to become under-inclusive over time; this argument is roughly equivalent to the flexibility consideration I discuss here; and (3) institutional competence (*Id.* at 1694), by which he refers to the relationship between the executive branch and the legislature and does not address the judiciary. Ohm then criticizes each of these arguments and concludes supporting technology-specific legislation for surveillance law.

Bert-Jaap Koops pointed to four legislative purposes in opting for technological neutrality: (1) achieving specific results; (2) functional equivalence between different modes of activity; (3) non-discrimination between technologies that have the same effects; and (4) allowing for future technological developments, which is what I call here flexibility. Bert-Jaap Koops, *Should ICT Regulation be Technology-Neutral*, *in* STARTING POINTS FOR ICT REGULATION: DECONSTRUCTING PREVALENT POLICY ONE-LINERS 77 (Bert-Jaap Koops et al. eds., 2006). *See also* Chris Reed, *Taking Sides on Technology Neutrality*, 4(3) SCRIPTED 263, 268 (2007).

technologies in detail, and once we acknowledge that technology does develop and change faster than the pace of the legislative process, the preference for a law that will last for longer than the present moment is clear. Bert-Jaap Koops called this the "futureproofing" of the law.[37] A law that mentions a specific technology is bound to become obsolete sooner rather than later, whereas a law that does not name a particular technology might be able to apply to the next innovation. Instead of naming technologies, technology-neutral legislation focuses on its functions or on the related human behavior. Such legislative flexibility also answers the argument often raised by the technology-separatist view discussed *supra*, which is that the law itself is obsolete and that its attempts to regulate technology are doomed to fail.

Legislators of a flexible, technology-neutral law rely on others to interpret the law and apply it to particular concrete circumstances. Regulators in the executive branch often apply the law to specific cases, as do courts. It is a regular judicial task to interpret a law and apply it to new technologies that emerged after the law was enacted.

Surveillance law provides an example of the needed legislative flexibility and the courts' ability to apply general, technology-neutral laws to concrete technologies.[38] Orin Kerr suggested that the technology-neutral Fourth Amendment should be transposed to the Internet.[39] His suggestion leaves the law technologically neutral and asks the courts to conduct the application in a technology-neutral manner as well.[40] Other than the Fourth Amendment itself, current American surveillance legislation is technology-specific: each law is based on a specific kind of technology—postal mail, telephone, e-mail, etc.[41] Thus, courts need to interpret each factual situation to fit it to the relevant

---

[37] Koops, *supra* note 36.

[38] *But cf.* Ohm, *supra* note 29 (arguing in favor of technology-specific surveillance laws).

[39] *See* Orin S. Kerr, *Applying the Fourth Amendment to the Internet: A General Approach*, 62 STAN. L. REV. 1005 (2010). Kerr discusses the inside/outside distinction regarding a physical setting under Fourth Amendment jurisprudence and suggests that courts roughly replicate it in the digital environment. The equivalent he suggests is content/non-content regarding communications networks.

[40] *Id.*

[41] *See* Robert A. Pikowsky, *An Argument for a Technology-Neutral Statute Governing Wiretapping and Interception of E-Mail*, 47 THE ADVOCATE 23 (2004) (advocating a unified level of protection of communications, regardless of the technology).

statute.[42] For example, before the enactment of the Electronic Communications Privacy Act of 1986 (ECPA), courts struggled to place mobile (not yet cellular) cordless phones within the legislative scheme.[43]

In privacy law, the Video Privacy Protection Act of 1988 (VPPA) applies to "video tape service provider[s]."[44] While the term "video tape" is left undefined, the definition of the service provider is a bit broader and covers "prerecorded video cassette tapes or similar audio visual material."[45] Paul Schwartz considers this definition to be a technology-neutral one, which easily covers DVDs,[46] yet he admits that technological convergence raises new challenges, and that there are open questions if the VPPA is to apply to digital media.[47] The legislative text addresses content which is fixed in a tangible medium, to borrow a term from copyright law, but it also adds "similar audio visual material." It took a court decision to conclude that online video content falls within the VPPA's definitions.[48] The district court explained that the VPPA is about the video content, not the method of delivery of the content.[49] The court then concluded that "Congress used 'similar audio video materials' to ensure that VPPA's protections would retain their force even as technologies evolve."[50] In other words, the court read the statute as technologically neutral.

These examples of surveillance law and the VPPA demonstrate how the law can be technology-neutral on one level but at the same time technology-specific in practice. Moreover, the examples illustrate that courts can stretch old technological definitions to apply to newer technologies, but only to some extent.

---

[42] If the technology-specific laws do not cover all situations, courts might struggle first to find the appropriate statute and then apply it to the concrete situation. This is for example the current state of surveillance law in Israel. Courts struggle with classifying email communication into the Secret Monitoring Act of 1979 and ask questions such as: "When was the conversation completed? If it was intercepted before the recipient opened the email box, is it subject to regular search and seizure rules or to the Secret Monitoring Act?" *See, e.g.*, CrimA 040206/05 State of Israel v. Philosoph [2007] (Isr.) (unpublished opinion) (on file with the author).

[43] *See* Pikowsky, *supra* note 41, at 25.

[44] Video Privacy Protection Act, 18 U.S.C. § 2710 (2006). Congress enacted yet another law referring to personally identifying information collected by a cable operator with respect to the subscriber. *See* Cable TV Privacy Act, 47 U.S.C. § 551 (2006).

[45] 18 U.S.C. § 2710(a)(4).

[46] Paul M. Schwartz, *Preemption and Privacy*, 118 YALE L.J. 902, 912 (2009).

[47] *Id.* at 923.

[48] *See* In re Hulu Privacy Litig., No. 11-03764, 2012 WL 3282960 (N.D. Cal. Aug. 10, 2012).

[49] *Id.* at *5.

[50] *Id.* at *6.

In the context of patent law, Dan Burk and Mark Lemley pointed to the legislative neutrality of the law, but argued that "[a]s a practical matter, it appears that while patent law is technology-neutral in theory, it is technology-specific in application."[51] The technological neutrality of patent law enabled it to remain relevant for over two centuries since the ratification of the Constitution granted Congress the power to enact such laws,[52] and despite technological advancements and the shift from mechanical inventions to electronics, computing, telecommunications, and biotechnology.[53] More specifically, Burk and Lemley pointed to the patent law doctrine of the "person having ordinary skill in the art" as the legal place that enables the general technology-neutral law to be applied in a specific manner.[54] Still in patent law, Michael Meurer focused on the utility requirement and argued that although it is phrased in a technology-neutral language, it is relevant only for biotechnological inventions.[55] However, the utility requirement does not impede any other inventions on their way to be protected by a patent.[56]

The cases taken together indicate that one prevalent legislative technique is to have a division of labor between the legislature and the judiciary, utilizing the technology-neutral stance. Opting for a technology-neutral legislative technique shifts some power from the legislature to the courts. There is also an important difference in the timeline: the general, technology-neutral law is an *ex ante* regulation, while the specification and application of the general instruction to the facts of the case is conducted *ex post*, on a case-by-case basis.

The flipside of flexibility does not only opt for present and specific technologies, but also certainty. A technology-specific legislation is almost by definition more accurate and specially tailored to the problem that the legislation aims to solve. It can pin-point the issues at stake in a particular context.[57] A technology-

[51] Dan L. Burk & Mark A. Lemley, *Is Patent Law Technology-Specific?*, 17 BERKELEY TECH. L.J. 1155, 1156 (2002). But, at least regarding the one patent law doctrine, there is an argument that the law is applied in a neutral way. *See* Kevin Emerson Collins, *Semiotics 101: Taking the Printed Matter Doctrine Seriously*, 85 IND. L.J. 1379, 1419 (2010) (arguing that courts formulated the printed matter doctrine in a technology-neutral way).

[52] U.S. CONST. art. I, § 8, cl. 8.

[53] Burk & Lemley, *supra* note 51, at 1159.

[54] Burk & Lemley, *supra* note 51, at 1185-90.

[55] Michael J. Meurer, *Patent Examination Priorities*, 51 WM. & MARY L. REV. 675 (2009).

[56] *Id*. at 706 ("On its face, the utility standard is technology neutral, but in practice the utility standard is usually an issue for only chemical inventions.").

[57] See the following arguments in favor of technology-specific laws, which turn to the need for nuanced, tailor-made laws. In the context of surveillance law, Ohm, *supra* note 29, at 1695-96, argues that some technological differences do

specific legislation is less flexible, but on occasion we do prefer accurate, narrowly-tailored regulations. For example, when the law is restrictive and might have adverse consequences, a specific legislation is preferable. This is the case with law that might have a chilling effect on innovation (an issue discussed below) or on speech. It might also be the case that the legislature prefers a cautious, step-by-step approach instead of attempting to instate a more general approach. Caution is advisable when the technological path is particularly ambiguous, mysterious, and unexpected, such as in the case of nanotechnology, at least at this point in its research.[58]

Those who, for constitutional reasons, prefer that law-making remains the task of the legislature rather than the judiciary also tend to favor technology-specific legislation that gives the judiciary a narrower role. Paul Ohm lists a related constitutional consideration in favor of technology-specific legislation: technology-specific laws limit the executive branch's power so that if new technologies require rethinking the law, it will be Congress that will examine the matter, in an open, transparent, participatory way, rather than the executive branch.[59]

2. Innovation

The legislative technique regarding technology interacts with an important consideration in technology policy: innovation. The baseline is that society is interested in promoting innovation. Innovation is a complex notion,[60] which requires separate treatment; here I will assume that it is a public interest.

---

deserve different treatment. In the context of nanotechnology, Susan Brenner argues for a technology-specific regulation "given the apparently unique aspects of the technology at issue," but she also raises some doubts, as she assumes that a specific law would result in a specialized regulator even though it is too early to assess whether the technology would be a transformative one. *See* Susan W. Brenner, *Nanocrime?*, 2011 U. ILL. J.L. TECH. & POL'Y 39, 56 (2011). In the context of RFID, Hildner, *supra* note 29, at 163-65, argues that technology-specific laws are justified on the grounds that "[t]echnology-specific legislation allows for collection limitation provisions particular to RFID, which makes it more rigid than baseline privacy legislation but also more nuanced," and that it is tailored. Hildner assumes that the general privacy legislation lacks such a collection limitation principle, which need not necessarily be the case. However, the EU does have such a principle. *See* Council Directive 95/46, *supra* note 1, art. 6(1)(b).

[58] *See* Brenner, *supra* note 57, at 56-57.

[59] *See* Ohm, *supra* note 29, at 1686, 1700.

[60] *See* Gaia Bernstein, *In the Shadow of Innovation*, 31 CARDOZO L. REV. 2257 (2010) (arguing that the innovation discourse draws our attention to the beginning of the life cycle of a technology and away from its diffusion).

Technology-specific legislation might hinder innovation in at least three ways.

First, if the law chooses one technology, the incentive to develop other technologies that achieve the same function might decrease. For example, in the context of electronic signatures, had the law chosen a particular technology as the only legal way to validate the e-signature, there would be less incentive for competitors to develop another technology that might be superior.[61] A technology-neutral choice, on the other hand, encourages competition among developers and among technologies. It creates a breathing space for innovation.[62] If we end up with several technologies, we might need to solve the question of interoperability, but so far the market has proved that it can handle this, on occasion with legal support in the form of antitrust law.[63]

Second, a legislative endorsement of one particular technology might cause a technological lock-in: the chosen technology will be used even if there are superior technologies. Once a technology is implemented and widely used, there are costs of switching to other technologies (e.g., costs of removing the old technology, installing the new one, learning to use the new one, converting old outputs to the new technology). If the switching costs are higher than the perceived benefit, a technological lock-in would occur, even though the locked-in technology is inferior to newer ones.[64] A technology-neutral law reduces the chances of a

[61] For a similar argument in the context of environmental law, see Nicholas G. Morrow, Note, *Federal Regulation of Greenhouse Gas Emissions a Practical Certainty: How Will the Texas Energy Industry Survive--Maybe Thrive?*, 17 TEX. WESLEYAN L. REV. 237, 254-55 (2011), observing that a bill discussed there is not technology-neutral and adding that "many feel that because the Bill is not technology neutral, it steers energy companies away from developing renewable energy sources."

[62] "Breathing space? is a term borrowed from First Amendment jurisprudence, though it plays differently in each context. In the First Amendment context, breathing space is asserted in order to require a narrow legislation (or none at all), whereas in the context of innovation, breathing space requires flexible, broad legislation (or none at all). *See, e.g.*, NAACP v. Button, 371 U.S. 415, 433 (1963) ("Because First Amendment freedoms need breathing space to survive, government may regulate in the area only with narrow specificity.").

[63] In the famous Microsoft antitrust case, the company, which had a monopoly in one market (PC operating systems), tied to it a separate product (the Internet Explorer browser). One element of the decree against Microsoft was that it should disclose some proprietary information so as to enable third party developers to access it, in order to achieve interoperability. Mass. v. Microsoft Corp., 373 F.3d 1199, 1216-22 (D.C. Cir. 2004).

[64] The classic example is the arrangement of the keyboard in the QWERTY format, which was a result of a technological need of mechanical typewriters, but was carried on to electronic keyboards even though the mechanical problem

technological lock-in, although the market still might lead to such an unfortunate result. Once again, the technology-neutral legislative choice enables a breathing space for technological innovation. An innovation policy that relies *inter alia* on competition would like to avoid lock-ins of this kind. A technology-specific law encourages such lock-ins. While a neutral position might not necessarily avoid lock-ins, it at least does not support it.

Third, a technology-specific rule might provide incentives to work around the regulation. This might happen when the regulation imposes duties or legal liability on a party that operates or uses a specific technology. The savvy business or engineer will design the technology so to avoid the law's definition of the particular technology, thus avoiding the liability.

Technology-neutral legislation enables a breathing space for innovation and avoids the problem of being worked-around. On the other hand, the open-ended nature of a technology-neutral legislation might have a chilling effect on developers of technology. Not knowing in advance how the law might address their technology, they might refrain from pursuing it, perhaps to the detriment of all. Details and specification can provide certainty. Whether there is such a chilling effect requires empirical research; it would also depend on the attitude the law takes regarding the technology, namely whether it is permissive or restrictive.

3. Harmonization

A third consideration that supports technology-neutral legislation is that it is likely to achieve harmonization among different jurisdictions. This consideration applies when the technology or its use is not limited to a defined locality and where various jurisdictions address the same issue more or less simultaneously. Thus, this consideration is obviously relevant for the online digital environment. In this sense, the legal network converges with the network dimension, which characterizes many technologies. In the United States, harmonization is a relevant consideration when addressing laws that have or might have an interstate effect or when contemplating interstate federal legislation. In the European Union, it is relevant to achieve harmonization of the internal economic market.

The case of electronic signature, mentioned above, illustrates this point. Online transactions often take place across borders. Had each state chosen a particular technology and enacted

---

was no longer relevant. *See* Paul A. David, *Clio and the Economics of QWERTY*, 75 AM. ECON. REV. 332 (1985).

it into its legislation in a technology-specific manner, then, inasmuch as electronic signatures are important to facilitate online commerce, there would likely be an impediment to interstate and international e-commerce.[65] A technology-neutral legislation would validate many technologies, not based on their specificities but on their function, and thus enable harmonization.[66] The downside of opting for a broader statutory language is that the use of many different technologies might lead to lack of interoperability.

Thus, the greater the importance we attach to harmonization, the more general the law would be, namely, opting for less specificity and more neutrality.

C. An Initial Typology

The considerations discussed above might justify a technology-neutral legislative technique, but this is only the first of a series of decisions to make. The choice of a legislative technique is not necessarily crude, between a technology-neutral position and a technology-specific one. We should take into account a broader range of parameters, resulting in a richer matrix of legislative choices. The dichotomy is thus replaced with several continuums that can help us nuance the legislative decision. *First*, what does the law regulate? What is the place of the technology in the specific legislation? Is the technology the law's subject matter or is the technology just a tool? *Second*, how does the law treat technology? Does the law actively promote, passively permit or directly restrict it? *Third*, how does the law define the regulated technology? What is the level of abstraction in which the legislation treats the technology? *Fourth*, who regulates technology? What body assumes the task? We can then examine if and how the considerations of flexibility, innovation and harmonization intertwine with the suggested continuums.

1. What does the law regulate? Ends—Means

In some cases, technology is at the center of legislation. It is its subject matter. This is the case, for example, with intellectual property law. In other cases, the subject matter of the legislation is not the technology per-se, but a different subject, such as

[65] Indeed, early state laws on electronic signatures were technology-specific, but these were preempted by a federal law in 2000. *See* Allison W. Freedman, Note, *The Electronic Signatures Act: Preempting State Law by Legislating Contradictory Technology Standards*, 2001 UTAH L. REV. 807.
[66] *See* Raymond, *supra* note 28, at 29.

preventing copyright infringement, facilitating e-commerce or assuring children's privacy. When technology is an inevitable part of the legal field it might be treated directly or indirectly as a means to achieve such ends. Below are some examples.

Patent law places technology at center-stage. It is meant to "promote the progress of science and useful arts,"[67] and regulates "any new and useful process, machine, manufacture, or composition of matter."[68] Patent law is about encouraging new inventions in all technological fields. We might debate what a technology means in this context— for example, we might wonder whether a method of doing business qualifies as an invention.[69] Ultimately, once we agree on what qualifies as a technological field, patent law is geared towards technology. Technology is the law's end. The forward-looking approach, actively encouraging technological innovation, demands a technology-neutral approach. The general and neutral law becomes concrete and technology-specific when the Patent Office examines applications or when courts apply the law.[70] If the government is interested in a particular technology it can always offer other incentives, such as procurement, direct investment, subsidies, or tax deductions.

Copyright law also focuses on technology, but with less intensity than its sister field of patent law. Copyright law is said to encourage originality (and arguably, also creativity) in arts and literature.[71] Once we accept the basic principle of copyright law, that it protects original expressions rather than ideas,[72] we realize that expressions come in various shapes and sizes, according to the technology used. It can be written text, photograph, sculpture, broadcast, television or film, digital content, and much more.[73] In

[67] U.S. CONST. art. I, § 8, cl. 8.
[68] 35 U.S.C. § 101 (2006).
[69] *See* Bilski v. Kappos, 130 S. Ct. 3218 (2010) (holding that methods of doing business are not categorically outside the scope of patent law).
[70] *See* Burk & Lemley, *supra* note 51, at 1156.
[71] *See* U.S. CONST. art. I, § 8, cl. 8.; Feist Publ'ns, Inc. v. Rural Tel. Serv. Co., 499 U.S. 340, 345 (1991) (holding that originality is the *sine qua non* of copyright law).
[72] *See* 17 U.S.C. § 102(b) (2006).
[73] In this sense, contemporary copyright law is technology-neutral in that it is not limited to a specific medium or technology. Yet, American copyright law does require that the original expression is "fixed in any tangible medium of expression now known or later developed." *Id.* Despite its future-welcoming approach, the fixation requirement could be seen as a technological limitation, as temporary copies are not fixed in a tangible medium, nor are oral lectures, unless they are based on a written text or recorded in some way. For a discussion of the judicial treatment of the fixation requirement regarding RAM temporary copies, see Melissa A. Bogden, *Fixing Fixation: The RAM Copy Doctrine*, 43 ARIZ. ST. L.J. 181 (2011).

fact, the history of copyright law indicates that it advanced step by step, following new technologies.[74]

Mapped onto the three considerations mentioned above, patent law and copyright law are, firstly, interested in maintaining flexibility as to the forms of inventions and creative works, in order to achieve innovation (patent law) and creativity (copyright law). Secondly, the neutrality enables a breathing space for innovation and creativity. Thirdly, a technology-specific law would cause difficulties in the international market, as different countries would end up protecting different kinds of inventions and works; hence the consideration of harmonization also pulls towards a technology-neutral stance.

On the users' side, we do see that the neutrality is sometimes compromised: in jurisdictions such as the EU that opted for an enumerated list of exceptions, subject to a general "three step test," some of the exceptions are technology-specific.[75] However, in jurisdictions that opted for an open-ended, standard-form fair use defense (e.g., the United States, Israel and the Philippines), copyright law is technology-neutral.[76]

When we turn to e-commerce law, the subject matter and goal of the legislation is to facilitate and promote various forms of commercial interactions. Technology enables and forms the environment where such interactions take place, but from a legislative point of view, technology serves as a means rather than an end in itself. A leading example is the electronic signature mentioned *supra*; e-signatures play an important role in facilitating and streamlining transactions as they enable the parties to authenticate the identity of their counter-parties. A law governing the signature adopts the e-signature itself as its subject matter. However, underlying the law is the functional role of the signature: e-signatures are regulated because of their role in facilitating e-commerce, not because e-signatures have some inherent social value. The function (facilitating e-commerce) is more important than the technology's essence. All three considerations—

---

[74] *See, e.g.*, STUART BANNER, AMERICAN PROPERTY: A HISTORY OF HOW, WHY AND WHAT WE OWN 26 (2011) (discussing the growth of copyright law along new forms of expression).

[75] *See* Guido Westkamp, *The 'Three-Step Test' and Copyright Limitations in Europe: European Copyright Law Between Approximation and National Decision Making*, 56 J. COPYRIGHT SOC'Y U.S.A. 1, 20 (2008) ("The permissible limitations are partially formulated in a technology-neutral manner and partially dependent on the [sic] whether the resulting copy is 'digital.'").

[76] *See* 17 U.S.C. § 107 (2006); Copyright Act of 2007, 5768-2007, 2007 LSI 38, § 19 (Isr.); Intellectual Property Code of the Philippines, Rep. Act No. 8293, § 185 (June 6, 1997) (Phil.).

flexibility, innovation and harmonization—demand a technology-neutral law.[77]

A caveat is in place: the line between presenting a law's treatment of technology as an end or as a means is not a firm one, but neither is such a description natural or inevitable. We can describe patent law as promoting human flourishing and thus treat technology as a means to achieve it. We can describe copyright law as an "engine of free expression"[78] and thus relegate technology to a secondary role. We can describe e-commerce legislation as an attempt to regulate technology directly. Indeed, the above presentation of the role of technology is not the only one possible. It is important, however, that legislatures and policymakers recognize that there are various roles to which they can designate technology in each context. Once they do so, they can evaluate the considerations for or against a technology-neutral approach and make an informed decision. It is a legislative choice.

2. How does the law treat technology? Promotion—Restriction

The law can promote a technology, permit it, be indifferent to it, discourage it, or even restrict it. Thus, there is a spectrum of attitudes that the law can take regarding a technology. We can place various laws on this spectrum.

Patent law is a case of the law promoting technology. In its legal sister, copyright law, the picture is more complex. Copyright law's anti-circumvention rules prohibit the manufacturing of a technology that is primarily designed for the purpose of circumventing a technological measure that controls access to a copyrighted work.[79] In plain language: the law prohibits breaking a technology that protects a copyrighted work, such as a password-protected digital music file. There are two technologies here: one is the technology that protects the copyrighted work (the "technological measure"); the other is the circumventing technology. The law's attitude to the former is at least passive-permissive, as it allows its use but does not require it, though we can go further and say that by protecting it, the law promotes the use of such technologies. As for circumventing technology, the law takes a prohibitive stance. Note that both kinds of technologies are described in a neutral language, based on their functions, rather than naming any particular technology or kind of technology.

---

[77] Raymond, *supra* note 28, at 33.
[78] I borrow the term from Harper & Row Publishers, Inc. v. Nation Enters., 471 U.S. 539, 558 (1985).
[79] 17 U.S.C. § 1201(a)(2)(A) (2006).

We could examine additional laws and classify their treatment of technology on this spectrum. For our purposes here, what matters is the interaction of the axis of promotion—restriction with the consideration of innovation mentioned above. Legislatures may choose rules that reach all technologies or few. Technologies promoted will evolve and spread; technologies restricted will lag. If the legislature is interested in promoting technology at large (as in patent law), a technology-neutral language allows maximum leeway for innovation. On the other hand, if the law restricts or prohibits a technology — a rare situation but one that does exist (regarding the production of weapons, drugs, malware or copyright anti-circumvention technologies, for example), then neutral language will lack certainty and might have a chilling effect on other technologies. In the case of a prohibition against weapons of mass destruction, perhaps such a chilling effect is a good idea, but in the case of copyright law, a broad prohibition of anti-circumvention technologies might deter the development of new technologies which have, as is often the case, a dual use: one that is innovative, creative and legal, and another that circumvents the protective technological measures and facilitates infringement.[80] On the other hand, a narrow, technology-specific law will be quite useless, as it will be easy to design a new technology around the statutory limitations.[81]

Once again, the legislature has a choice and it should be informed, *inter alia*, by the relevance of the three considerations of flexibility, innovation and harmonization, and their interplay with each possible point on the legislative yardstick.

3. How does the law define the regulated technology? Abstract—Concrete

A law can define the technology at stake in several levels of abstraction. Thus, as in the previous parameters, the choice between a technology-neutral and a technology-specific legislation is not a binary dichotomy, but a continuum. We can assume, for the sake of illustration, a law that permits the use of a particular version of particular software for a certain purpose. Such a detailed instruction might appear in a technical guide, but it is unlikely to

[80] The anti-circumvention rules, added to the Copyright Act by the DMCA in 1998, were criticized *inter alia* for their limitation of innovation. *See* Niva Elkin-Koren, *Making Technology Visible: Liability of Internet Service Providers for Peer-to-Peer Traffic*, 9 N.Y.U. J. LEGIS. & PUB. POL'Y 15, 72 (2005).

[81] It is not only "pirates" that carefully work around specific rules. Law enforcement might use new technologies that do not trigger technology-specific privacy protections. For this argument, see DANIEL J. SOLOVE, NOTHING TO HIDE: THE FALSE TRADEOFF BETWEEN PRIVACY AND SECURITY 170-71 (2011).

appear in legislation. At the other end, patent law treats technology in the broadest possible manner (or so it seems at first sight).[82] In between these ends, there are numerous levels of abstraction. Consider again copyright law's anti-circumvention rule. Both technologies mentioned there (the copyright protective technological measure and the circumventing technology) are not specified in detail; rather, they are described according to their function (protect a copyrighted work; circumvent a technological measure). Legislatures can choose the level of abstraction.

American free speech jurisprudence provides a useful terminology that we can borrow in order to better understand the legislative options. Courts subject limitations of speech to different degrees of scrutiny. The key is whether the limitation (a statute, executive decision, etc.) is content-based or content-neutral. If it is the former, the limitation would be reviewed under strict scrutiny, meaning that it is presumptively unconstitutional, unless the government shows otherwise.[83] Content-neutral regulation is subject to an easier, intermediate scrutiny and is more likely to survive.[84] Courts developed a further distinction within the content-based category, asking whether the limitation of free speech is viewpoint-based or viewpoint-neutral.[85]

Borrowing this terminology, a better description of copyright law's anti-circumvention rules is that they are the equivalent of a "content-based but viewpoint neutral," category, as the law defines them according to a particular function but does not dictate a particular technology.[86] This analogy to free speech jurisprudence enables us to see first, that the neutral/specific distinction is not a binary one, and second, that we need to be more accurate in describing the law.

---

[82] Meurer, *supra* note 55, at 706.

[83] *See, e.g.*, R.A.V. v. City of St. Paul, 505 U.S. 377, 382 (1992).

[84] *See* Turner Broad. Sys., Inc. v. FCC, 512 U.S. 622, 642 (1994) (explaining the doctrine of content neutrality and applying it to must-carry rules in the telecommunications sector).

[85] *See e.g.*, Burson v. Freeman, 504 U.S. 191, 214 (1992) (Scalia, J., concurring); *R.A.V.*, 505 U.S. at 430 (Stevens, J., concurring). For a critical discussion, see Erwin Chemerinsky, *Content Neutrality as a Central Problem of Freedom of Speech: Problems in the Supreme Court's Application*, 74 S. CAL. L. REV. 49 (2000).

[86] In the case of copyright law, we can argue that the anti-circumvention rules are a violation of speech, which would call for the direct application of the content-based/content-neutral distinction. See my argument in Michael D. Birnhack, *Copyright Law and Free Speech after* Eldred v. Ashcroft, 76 S. CAL. L. REV. 1275, 1314, 1316, 1330 (2003). Netanel made a similar argument regarding the Copyright Term Extension Act of 1998. *See* Neil Weinstock Netanel, *Locating Copyright Within the First Amendment Skein*, 54 STAN. L. REV. 1, 5 (2001). In the context of privacy, the reference to free speech doctrines is as an analogy, not a direct application thereof.

4. *Who regulates technology?*

A final relevant parameter, echoing the consideration of flexibility in choosing the suitable legislative technique, is questioning who sets the rules and who applies them. The candidates are the legislature, the executive branch—a regulator of a specific sector in most cases[87]—and the judiciary.

A typical structure is that the law is technology-neutral in text but becomes specific in application. The specification can be based on the kind of technology, or it can address a specific technology. This is, for example, the case in patent law and surveillance law, mentioned above.[88] In such cases, there is a constitutional division of labor between the legislature and the judiciary, which might mitigate some of the criticism voiced against the technology-neutral position. The *ex post* specification by the courts adds certainty and foreseeability, thus minimizing the chilling effect, if one exists.

D. Interim Summary

There are three main considerations that legislators should weigh when drafting legislation and choosing a legislative technique: flexibility, innovation, and harmonization. If these three considerations apply to the circumstances of a particular issue, they can justify the choice for technology-neutral legislation. Once a legislature opts for a neutral position, there are further choices to make. Instead of a binary choice of all or nothing, I argued that there are several continuums available that provide a richer set of options: a law can treat technology at any point on the end—means spectrum, the promotion—restriction spectrum, and the abstract—concrete spectrum, and it can allocate responsibility for different segments of these choices to different players in the legal field. Considering the best mode of legislative technique not in the abstract, but vis-à-vis the matrix of possibilities, can yield more nuanced options and hopefully better results.

However, in practice, we see that technology-neutral legislation is often preferred *a-priori*, without considering the various justifications and parameters discussed above. The advantages of neutrality are taken for granted. Laws are phrased in a neutral way and the legislators present them as such. But returning to the paradox presented at the outset of this article: is

[87] Susan Brenner points to the current state of the law regarding nanotechnology. There is no one law that addresses it, but there are three federal agencies that claim authority to regulate certain aspects thereof. *See* Brenner, *supra* note 57, at 50.

[88] *See, e.g.*, Burk & Lemley, *supra* note 51; Kerr, *supra* note 39.

neutrality possible at all? We should ask this question when the legislature strives for legislative neutrality, either intuitively or after a thorough deliberation. To better understand this question, I suggest that we reverse engineer the law, to which I now turn.

III. REVERSE ENGINEERING THE LAW

Some laws reveal their technological mindset, as they address a specific technology directly. There is not much need to reverse engineer such laws (unless we are suspicious about the statutory statements): what we see is what we get. A law that would regulate Radio Frequency Identification (RFID) tags exclusively (there is no such law that I am aware of) would assume the RFID technology. Other laws attempt, whether self-consciously or not, to conceal their technological mindset. One way to do so is to draft the legislation in a technology-neutral manner, so that it applies not only to one particular technology but to other known or future technologies as well. However, such a position means that the law tries to resist its own biases and its own technological mindset. Is it possible for the law to think beyond the current state of the art? The challenge for the legislators is to realize the limits of technological neutrality; the challenge for the researcher is to examine the validity of the claimed neutrality. This Part undertakes the latter task and offers a general mode of statutory interpretation, tailored to technological contexts.

Technology-related laws assume a technological context. Otherwise, they would be superfluous. Contract law has an underlying vision of how contracts are formed or should be formed. Without such a vision regarding its subject matter, contract law would be an incoherent set of arbitrary rules. Criminal law reflects an understanding of crime, harm and punishment. Without such a vision, criminal law would be nothing but the sovereign's arbitrary and capricious command. We can go on to consider other fields of law: what is each field's vision regarding its subject matter? Rarely is it explicitly stated, but it is always present.

As the examples of contract law and criminal law illustrate, it is often the case that the law's vision about its subject matter is not explicit. Moreover, the law's underlying mindset about its subject matter might be biased in one way or another, be incoherent, or simply wrong. Imagine contract lawyers trying to answer the question about the law's underlying perception of how contracts are formed. To figure out the hidden assumptions, we should look deeper.

Moreover, every field of law has a vision as to technology. Contract law, for example, holds various technological assumptions about the means of communications of the parties (oral/writing, synchronous or asynchronous), the formation of the contract (shaking hands, signing documents or exchanging emails) and its form (oral, written, digital). Here, I focus on laws that address technology more directly. The law in general, and technology-related laws in particular, holds a hidden technological assumption.[89] Katherine Strandburg argues, for example, that the Fourth Amendment, drafted with the idea of a physical home in mind, should be extended to cover the networked world. She implies technosocial continuity, which "consider[s] the intertwined effects of technological and social change."[90]

This is where reverse engineering of the law enters the picture. It is an interpretive methodology that can assist us in uncovering the hidden assumptions of the law about technology. The metaphor of reverse engineering is borrowed from computer science and trade secret law. It is inspired by the rich jurisprudential discourse about interpretation of laws and hermeneutics and, more specifically, by one strand of literary criticism.

Computer scientists and engineers reverse engineer software and end-products, with the intention of figuring out how the product was designed and what its internal logic, mechanism and underlying ideas are. Reverse engineering begins with the end-product rather than with the original code or design and works backwards, in a reverse direction. Reverse engineering is done either because there is no access to the original plans (due to technological barriers or since it is kept secret) or because the process itself provides an important learning experience.[91] The underlying ideas and concepts are not protected by copyright law and they are often needed to achieve interoperability.[92] Trade

[89] *See* Harry Surden, *Structural Rights in Privacy*, 60 SMU L. REV. 1605 (2007) (arguing that the law often relies on latent structural constraints, which are physical or technological barriers which regulate conduct).

[90] Katherine J. Strandburg, *Home, Home on the Web and Other Fourth Amendment Implications of Technosocial Change*, 70 MD. L. REV. 614, 619 (2011); *see also* Orin S. Kerr, *An Equilibrium-Adjustment Theory of the Fourth Amendment*, 125 HARV. L. REV. 476 (2011) (arguing that Fourth Amendment jurisprudence reflects a judicial reaction to new technologies).

[91] The philosophy of the Free Software movement includes four freedoms, the second of which is "[t]he freedom to study how the program works." See *What is free software?*, FREE SOFTWARE FOUND., http://www.gnu.org/philosophy/free-sw.html (last updated July 2, 2012).

[92] *See* Sega Enterprises, Ltd. v. Accolade, Inc., 977 F.2d 1510, 1514 (9th Cir. 1992) (concluding that "when the person seeking the understanding has a legitimate reason for doing so and when no other means of access to the

secret law permits such reverse engineering.[93] A special defense in the Semiconductor Chip Protection Act of 1984 allows reverse engineering.[94] When the process requires temporary copying, copyright law's fair use defense (subject to its considerations) as well as specific statutory permissions might apply.[95] All of these legal mechanisms support reverse engineering.

Applying reverse engineering to the reading of the law means that we begin with the text of the legislation and work backwards, in order to decipher its conceptual building blocks. One way to uncover the foundations is to turn to external evidence. This is the kind of research that legal historians or political scientists often engage in. Reverse engineering the law is not interested in the history of the law *per se* (though historical analysis can be highly beneficial). Instead, it is interested in the end-product: what the legislators finally did regarding technology, not what they intended.

The parallel to the textualist mode of legal interpretation is obvious, but reverse engineering is not such a textualist exercise. Some jurists argue that the meaning of the law is confined to its text.[96] They refuse to query the original meaning of those who drafted the law and they firmly resist injecting contemporary ideas into the text. The textualist interpretation reads the plain text of the law and seeks other clues within the text for its meaning, such as the repeated use of terms, division into sections, etc. The textualist methodology reflects a long line of presuppositions as to the meaning of law, the authority of the interpreter, and much more.[97]

---

unprotected elements exists, such disassembly is as a matter of law a fair use of the copyrighted work").

[93] *See* California Uniform Trade Secrets Act, CAL. CIV. CODE § 3426.1(a) (West 1985), which lists reverse engineering as an example of proper means to acquire knowledge of a trade secret.

[94] *See* 17 U.S.C. § 906(a)(1) (2006).

[95] *See* 17 U.S.C. § 107 (2006) (fair use defense); *Sega Enterprises*, 977 F.2d 1510, 1520-21; and the exceptions to the anti-circumvention rules that allow reverse engineering under certain conditions for purposes of achieving interoperability, encryption research and security testing, 17 U.S.C. § 1201(f)-(h) (2006).

[96] *See, e.g.*, Antonin Scalia, *Common-Law Courts in a Civil-Law System: The Role of United States Federal Courts in Interpreting the Constitution and Laws*, *in* A MATTER OF INTERPRETATION: FEDERAL COURTS AND THE LAW 23 (Amy Gutman ed., 1997); Charles Fried, *Sonnet LXV and the "Black Ink" of the Framers' Intention*, *in* INTERPRETING LAW AND LITERATURE: A HERMENEUTIC READER 45 (Sanford Levinson & Steven Mailloux eds., 1988).

[97] For a critical discussion, see Paul Brest, *The Misconceived Quest for the Original Understanding*, *in* INTERPRETING LAW AND LITERATURE: A HERMENEUTIC READER, *supra* note 96, at 69. Other interpretive modes do not necessarily ignore the text; quite to the contrary, but they focus on the text in

The text-based interpretation has practical implications, as it serves those who apply it to determine what the law is.

Reverse engineering the law applies some of the same tools used by the textualists, in that it confines itself to the text of the legislation, it does not seek the history of the law, and it does not turn to other external evidence about the meaning of the law. But the reverse engineering of the law does not rule out alternative modes of interpretation and does not have a normative claim of exclusivity; in fact, it does not have any normative claim (other than the assumption that the law reflects a technological setting). The reverse engineering is a tool in the service of description: it is interested in exposing underlying technological assumptions that were built in the law or that the law was built around. In this sense, the reading I propose here searches for the law's technological mindset rather than the mindset of its drafters.

Reverse engineering the law has closer affinity with the *New Criticism* strand in literary criticism, which focused on the text.[98] The interpretive convention that pre-dated the new criticism focused on the authors and their intentions. The new critics shifted the search for the meaning of the text from the author to the text itself. In order to figure out the meaning of a poem, a story, etc., the new critics refused to query the author's intentions. Neither did they examine the way in which the text was received by the readers. Audience-based theories of interpretation appeared only later in the day.[99] The new critics' interpretive tool was a close reading, searching for internal structures of the text.[100]

Reverse engineering the law thus begins with the text and tries to uncover the technological mindset, as reflected in the law. Reverse engineering the law does not insist on interpretive exclusivity. For example, it does not object to a historical analysis. It might not always provide us with a meaningful conclusion. But reverse engineering does carry potential explanatory power as to how the law thinks of the technology it regulates; it can teach us about the limits of the current law and provide us with some guidance as to the future.

It is now time to return to the paradox that drives the current inquiry, which challenges the very possibility of

---

relation to other interpretive nodes, such as the author of the text. *See, e.g.*, Ronald Dworkin, *The Arduous Virtue of Fidelity: Originalism, Scalia, Tribe, and Nerve*, 65 FORDHAM L. REV. 1249, 1254 (1997).

[98] For the New Criticism (or La Nouvelle Critique, in its French appearance), see, for example, TERRY EAGLETON, LITERARY THEORY: AN INTRODUCTION 38-42 (2d ed. 1996).

[99] *See* ROLAND BARTHES, IMAGE, MUSIC, TEXT (1978).

[100] *See, e.g.*, EAGLETON, *supra* note 98.

technology-neutral laws. I shall examine this by turning to the case study of informational privacy law: is this body of law technology-neutral? Does the law have an underlying technological mindset despite its purported neutrality? I first draw the legal framework of informational privacy and then reverse engineer the law.

IV. INFORMATIONAL PRIVACY

Over the last four decades, we have witnessed the gradual emergence of a new legal regime addressing informational privacy. It is an offspring of the classical right to privacy, extending privacy beyond the tort of disclosing one's private life. As a theoretical concept, informational privacy covers certain interests in "our" "private" or "personal" data. These terms are controversial. Some jurisdictions, namely Europe, use an identification-based criterion to define personal data,[101] whereas other jurisdictions, namely the United States, use a content-based criterion. Although this is not a rigid distinction, from a legal and practical point of view, the informational prong of privacy law developed differently in the United States than in Europe, providing us with two main models: a sectoral approach in the United States and an omnibus one in Europe, known as data protection law. The former model means that informational privacy is protected only in an enumerated set of cases, each protected by a specific (federal) law.[102] The latter model means that informational privacy is protected across the board, not only in a specific sector or context.[103]

---

[101] The identification criterion first appeared in the ORG. FOR ECON. COOPERATION AND DEV. (OECD), OECD GUIDELINES ON THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA OF 1980, §1(b) (1980) [hereinafter OECD GUIDELINES]: "'personal data' means any information relating to an identified or identifiable individual (data subject)." It was later adopted by the EU in its Data Protection Directive.

[102] *See, e.g.*, Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. No. 104-191, 110 Stat. 1936 (1996) (health-related data); Financial Services Modernization Act of 1999, Pub. L. No. 106-102, 113 Stat. 1338 (1999) (known as Gramm-Leach-Bliley Act) (financial data); Video Privacy Protection Act, 18 U.S.C. § 2710 (2006) (data about video rentals.); Family Educational Rights and Privacy Act of 1974 (FERPA), 20 U.S.C. § 1232g (2006) (data about students' records or information). There are only two federal informational privacy laws that have a general scope: the Privacy Act of 1974, 5 U.S.C. § 552a (2006), and the Children's Online Privacy Protection Act of 1998 (COPPA), Pub. L. No. 105-277, 112 Stat. 2581 (1998). The scope of the former is determined according to the context and the identity of the parties: the government and citizens. The scope of the latter is determined according to the age (under 13) of the data subjects.

[103] There are various explanations in the literature for the different approaches. James Whitman, following Robert Post, provided a political/philosophical explanation: the European legislative scheme is based on the idea of human dignity, whereas the American is based on the idea of liberty. *See* James Q.

This Part surveys the development of informational privacy/data protection as a legal category. The discussion provides the legal background for contemporary informational privacy law; explains the next Part's reverse engineering of European data protection law and enables us to elucidate from the discussion the recurring features of the emerging global informational privacy regime.

A. United States: Privacy and Private Information

The right to privacy is not enumerated in the Constitution or in the Bill of Rights. The founding fathers left privacy to the states and to the social realm, with the important exception of the Fourth Amendment, which regulates governmental searches and seizures. Privacy is further protected via other legal rights, such as the right to private property, copyright law in unpublished works and more.

As a legal right, privacy entered the common law with Louis Brandeis and Samuel Warren's famous 1890 Harvard Law Review article, *The Right to Privacy*.[104] Seventy years later, Dean William Prosser classified the judicial incarnations of the right to privacy into four torts,[105] later to be incorporated into the Restatement (Second) on Torts,[106] resulting in the wide diffusion of the privacy tort throughout the United States.[107] In the meantime, the right to privacy also gained power in the

---

Whitman, *The Two Western Cultures of Privacy: Dignity Versus Liberty*, 113 YALE L.J. 1151 (2004). Jon Mills points to the age of the American privacy law compared to the newly born EU; to the strength of freedom of speech in the United States, which trumps privacy; and to a stronger norm of governmental openness. *See* JON L. MILLS, PRIVACY – THE LOST RIGHT 273 (2008). Steven Salbu framed the legal discussion in the United States in terms of market-based solutions versus legislation and regulation. *See* Steven R. Salbu, *The European Union Data Privacy Directive and International Relations*, 35 VAND. J. TRANSNAT'L L. 655, 666-67 (2002). Helen Nissenbaum offers a theoretical support for the American sectoral approach to informational privacy. *See* HELEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE (2010). She proposes a comprehensive theoretical framework for privacy, which is anchored in social context. The context-based framework nicely fits the American sectoral approach, as a specific law for each sector can, at least potentially, be sensitive to the social context. *Id*. at 237-38. For critique, see Michael D. Birnhack, *A Quest for a Theory of Privacy: Context and Control*, 51 JURIMETRICS 447 (2011).

[104] Samuel Warren & Louis Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

[105] *See* William L. Prosser, *Privacy*, 48 CAL. L. REV. 383 (1960).

[106] RESTATEMENT (SECOND) OF TORTS § 652A (1997).

[107] For a critical assessment of Prosser's formulation of privacy torts, see Neil M. Richards & Daniel J. Solove, *Prosser's Privacy Law: A Mixed Legacy*, 98 CAL. L. REV. 1887 (2010).

constitutional context, namely in the relationship between state and citizen. The Supreme Court found that "various guarantees [in the Bill of Rights] create zones of privacy,"[108] and developed the right to privacy, mostly in two contexts. One was decisional privacy, referring to matters such as a woman's right to have an abortion,[109] and the second was Fourth Amendment jurisprudence.[110]

The early 1970s saw a new development in the United States. In 1973, an Advisory Committee to the Secretary of Health, Education and Welfare published a report (known as the Ware Report) that recommended regulating the collection and use of individuals' data by enacting a Federal Code of Fair Information Practice (FIP) for all automated personal data systems. Interestingly, in anticipating the discussion in the next Part, the committee was concerned first and foremost with the challenges of a particular kind of then-new technology: computer-based record keeping systems, or, in language that would become popular later, databases. The Secretary of Health, Education and Welfare, Caspar W. Weinberger, saw even further. His *Foreword* to the Report started with a technological vision: "Computers linked together through high-speed telecommunications networks are destined to become the principal medium for making, storing, and using records about people."[111] Note that this was in 1973 – only four years after the first distant computers were connected and long before we called it the Internet. It is also interesting to note Weinberger's formulation of the issue: he described the benefits of the computer-based systems in terms of powerful management tools, and the rival interests in terms of "protections of due process" rights.[112] He himself did not mention privacy, although the Committee did discuss privacy throughout the report.

The Ware Report listed five basic principles: (1) there should be no secret personal data keeping systems; (2) an individual should be able to know whether information about him is kept and for what purpose; (3) an individual should be able to

---

[108] Griswold v. Connecticut, 381 U.S. 479, 484 (1965).

[109] Roe v. Wade, 410 U.S. 113, 154 (1973).

[110] See Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring), which articulated the "reasonable expectations" test that triggers Fourth Amendment protection. For a recent application, see United States v. Jones, No. 10–1259, 2012 WL 171117 (U.S. Jan. 23, 2012), (finding that police attachment of a Global Positioning System (GPS) tracking device to an individual's vehicle and monitoring the vehicle's movements is a search within the meaning of the Fourth Amendment).

[111] Caspar W. Weinberger, *Foreword*: *Records, Computers and the Rights of Citizens: Report of the Secretary's Advisory Committee on Automated Personal Data Systems*, ELEC. PRIVACY INFO. CTR (July 1973), http://epic.org/privacy/hew1973report/foreword.htm.

[112] *Id*.

prevent data from being used for a purpose different from that for which the data was collected in the first place; (4) an individual should be able to amend a record of identifiable information about him; and (5) a duty should be imposed on the organization that collects or uses the data to assure the reliability of the data, its use for the limited-purpose and prevent misuse.[113] This was the debut of FIPs. In contemporary language, we can rephrase the principles slightly: (1) no secret databases; (2) a data subject's right to access his or her personal data; (3) limited-purpose principle; (4) a data subject's right to rectify incorrect personal data; and (5) duties of accuracy, limited purpose, and data security, imposed on controllers and processors of personal data.

A year after the Ware Report was submitted, with the Watergate scandal in the background, Congress enacted the Privacy Act of 1974, which regulates the disclosure of records on American citizens by governmental agencies.[114] This was the first federal law that provided explicit privacy protection to personal data.[115] While in the United States the introduction of FIPs was in the context of public law, framing the government-citizen relationship, the principles soon found their way to the private realm. Privacy was now discussed in new circles: the forum shifted from the local sphere to the international one. In the United States, the law remained within the confines of specific sectors. When, in 2011, the majority in the Supreme Court assumed, without deciding, that the Constitution protects a privacy "interest in avoiding disclosure of personal matters,"[116] Justice Scalia's concurrence clarified that "there is no constitutional right to 'informational privacy.'"[117]

B. The OECD and Data Protection in Europe

1. International Initiatives

[113] *Id*. Ch. III.

[114] Privacy Act, 5 U.S.C. § 552a (2006). The legislative history is 1466 pages long. *See* S. COMM. ON GOVERNMENT OPERATIONS & H. COMM. ON GOVERNMENT OPERATIONS, 94TH CONG., LEGISLATIVE HISTORY OF THE PRIVACY ACT OF 1974, S. 3418 (PUBLIC LAW 93-579): SOURCE BOOK ON PRIVACY (1976), http://www.loc.gov/rr/frd/Military_Law/pdf/LH_privacy_act-1974.pdf.

[115] Surveillance laws pre-dated the Privacy Act of 1974. Such laws regulated wiretapping and hence protected privacy interests. However, the interest was privacy in communications, rather than privacy in information per se.

[116] NASA v. Nelson, 131 S. Ct. 746, 751 (2011) (quoting Whalen v. Roe, 429 U.S. 589, 599-600 (1977)).

[117] *Id.* at 765.

In the meantime, several countries have already enacted laws regulating personal data.[118] In 1980 the OECD published its *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*.[119] With the growing global interest in informational privacy, the Council of Europe (CoE) offered the *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data* in 1981.[120] The Convention was also anchored in the main legal instrument of the CoE, the Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR) of 1950.[121] Article 8 thereof provides that "Everyone has the right to respect for his private and family life, his home and his correspondence."[122] Rephrased in the terms used here, the ECHR provides protection of privacy in several categories: informational privacy (private life), specific, content-based categories (family life), privacy in places (home), and privacy in communications (correspondence). The United Nations entered the picture in 1990, offering its *Guidelines for the Regulation of Computerized Personal Data Files* to all nations.[123] None of these international instruments were binding for any country (other than the CoE Convention, which applied to countries that chose to ratify it). The OECD and UN guidelines were recommendations, indicating a path and reinforcing FIPs.

---

[118] The German State of Hesse was the first (1970); Sweden followed by enacting a data protection law in 1973. See the brief account of the first data protection commissioner, Spiros Simitis, *Privacy – An Endless Debate?*, 98 CAL. L. REV. 1989, 1995-96 (2010). Other countries established expert committees recommending the enactment of such laws; for example in Canada (1972), UK (1972), and Israel (1981).

[119] OECD GUIDELINES, *supra* note 101, part 2. The Guidelines included eight principles: (1) data collection should be lawful and fair, with knowledge and consent where appropriate; (2) the data collected should be relevant to the purpose of its collection, accurate, complete and up to date; (3) the purpose of collection should be made at the time of collection and the data should be used for that purpose only; (4) the use should be limited to that purpose, with exceptions of the data subject's consent or a legal authority; (5) a duty of data security; (6) data subjects should be able find out about their data, its uses and about the data controller; (7) individuals' rights of access and rectification; and (8) accountability of the data controller.

[120] Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Jan. 10, 1985, E.T.S. No. 108.

[121] *See* Convention for the Protection of Human Rights and Fundamental Freedoms 1950, *opened for signature* Nov. 4, 1950, 213 U.N.T.S. 221 (entered into force Sep. 3, 1953), http://www.echr.coe.int/NR/rdonlyres/ D5CC24A7-DC13-4318-B457-5C9014916D7A/0/Convention_ENG.pdf.

[122] *Id*.

[123] G.A. Res. 44/132, U.N. GAOR, 44th Sess., Supp. No. 21, U.N. Doc. A/44/132, at 211 (Dec. 5, 1989).

2. *Enter the European Union*

The first to adopt the idea of protecting personal data as a comprehensive and binding legal regime was the European Community (EC), the predecessor of the European Union (EU). Several years of discussions resulted in the EU Directive on Data Protection of 1995.[124] The Directive has become the most powerful engine of promoting data protection on a global scale. It is binding on the EU's Member States, which were required to enact national laws that met the Directive's imperatives,[125] but its impact has reached beyond the borders of Europe.[126]

Overall, the Directive has two goals. One is the protection of data and the second, often overlooked or underestimated, is the facilitation of cross-border transfers of data. These two goals might seem to contradict each other, as the best way to enable cross-border data is not to attach any strings to it. The Directive attempts to calibrate a delicate balance between the two goals: it is a means to encourage commerce of personal data in a manner that protects the data subjects' rights.

The Directive provides a framework that imposes duties on those who handle the personal data and provides rights to the data subjects regarding their data, accompanied by some enforcement mechanisms. The basic principle is that personal data should be processed fairly and lawfully.[127] This overarching principle is then made more concrete in a series of specific limitations imposed on data controllers and rights accorded to data subjects. The key construct of the Directive is its definition of "personal data" (Art. 2(a)), which is based on an identification criterion rather than a content-based one.

The processing of personal data is allowed only if the data subject has unambiguously given his consent; in a few other situations where consent is inferred (as in the case of a contract); or for exogenous reasons, such as a compliance with a legal obligation, protecting the data subject, or carrying out a task that is in the public interest.[128] Further limitations include that personal data can be collected only for specific, explicit and legitimate purposes;[129] it should not be further processed in ways that are

---

[124] *See* Council Directive 95/46, *supra* note 1.

[125] The Directive does not directly apply in any of the legal systems of the EU member states. An Italian citizen, for example, cannot turn to an Italian court claiming her rights under the Directive were violated; she needs to point to the local Italian data protection law.

[126] *See* Birnhack, *supra* note 10.

[127] *See* Council Directive 95/46, *supra* note 1, art. 6(1)(a).

[128] *Id.* art. 7.

[129] *Id.* art. 6(1)(b).

incompatible with the original purposes;[130] the data collected should be adequate, relevant, and not exceed the data needed to fulfill the purpose of its collection;[131] and the data should be accurate and kept up to date.[132]

There are further requirements, including prohibition against processing some kinds of data—here the criterion is content-based: racial origins, political beliefs, health data, and sexuality are prohibited categories, with some exceptions based on the data subject's explicit consent.[133] The data controller is further subject to duties of confidentiality and data security.[134] The data subject's rights correspond to the duties of the controllers. In addition, the data subject has an independent right to access the data held by the controller about her,[135] to object to some processing,[136] and to object to automated decisions.[137]

The Directive and the legal regime of data protection it established were later anchored in constitutional grounds. Article 7 of the Charter of Fundamental Rights of the European Union of 2000 provides protection for privacy, stating "[e]veryone has the right to respect for his or her private and family life, home and communications."[138] Data protection deserved a separate constitutional status. Article 8(1) states that "[e]veryone has the right to the protection of personal data concerning him or her." Article 8(2) elaborates that

> Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.

A piece of supplementary EU legislation is the 2002 Directive on privacy and electronic communications as amended in 2009, often referred to as the e-Privacy Directive (hereinafter "e-Privacy Directive").[139] It addresses privacy issues specific to the

---

[130] *Id.*
[131] *Id.* art. 6(1)(c).
[132] *Id*. art. 6(1)(d).
[133] *Id.* art. 8.
[134] *Id.* arts. 16,17.
[135] *Id.* art. 12.
[136] *Id.* art. 14.
[137] *Id.* art. 15.
[138] Charter of Fundamental Rights of the European Union, 2000 O.J. (C 364), *available at* http://www.europarl.europa.eu/charter/pdf/text_en.pdf.
[139] Directive 2002/58, of the European Parliament and of the Council of 22 July 2002 Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector, 2002 O.J. (L 201) 37 (EC). The

telecommunications sector. For example, it requires providers of "publicly available electronic communications service" to secure their systems; [140] it sets a right to receive a non-itemized bill;[141] and regulates unsolicited communications.[142] In the terms provided previously in this article and to anticipate the following discussion, we can say that the e-Privacy Directive is technology-based. Although it does not name particular kinds of equipment or hardware, it is far from being technology-neutral. The definitions are on occasion at pains to describe a simple technology in a general manner. For example, the 2009 amendment refers to "the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user."[143] This seemingly broad definition covers cookies, spyware and viruses.[144] It uses open language, but its technological contours are quite specific.

3. The EU Directive: The Law Follows Personal Data

The Data Protection Directive has a unique mechanism to export itself to other jurisdictions beyond the borders of the EU. It allows the transfer of personal data on European citizens to non-EU countries only if the data receives a similar EU-level of protection in the country of destination.[145] Such a mechanism is important, as it prevents the bypassing of the local legal regime by way of foreign data havens.[146]

The Directive offers several mechanisms to ensure that the interests of European citizens are not compromised by a party located in a third country. The mechanisms include the consent of

---

Directive was amended in 2009, by Directive 2009/136 of the European Parliament and of the Council of 25 November 2009, O.J. (L 337) 11 (EC) [hereinafter *Amending Directive*]. The Amending Directive adds a duty to notify authorities and, if relevant, data subjects, of data breaches. The amendment also requires the user's consent before storing or accessing information in his or her terminal equipment – in other words, before using cookies. *Id.*

[140] Directive 2002/56*, supra* note 139, art.4.

[141] *Id.* art. 7.

[142] *Id.* art. 13.

[143] Amending Directive, art. 2(5), amending art. 5(3) of the e-Privacy Directive.

[144] *See id.* Recital 66 (listing these as examples).

[145] *See* Council Directive 95/46, *supra* note 1, art. 25.

[146] PETER P. SWIRE & ROBERT E. LITAN, NONE OF YOUR BUSINESS: WORLD DATA FLOWS, ELECTRONIC COMMERCE AND THE EUROPEAN PRIVACY DIRECTIVE 26 (1998).

the data subject (between the subject and a data controller),[147] standard contractual clauses (between two controllers),[148] or Binding Corporate Rules (for multinational corporations).[149] Yet another mechanism is more general in scope. It streamlines the data transfer to a third country if the law in that country provides an adequate level of protection. The EU conducts "adequacy assessments." Adequacy does not mean that the law in the third party is identical to the Directive.[150] This export mechanism means that the European law follows European personal data. It does not force itself onto other countries and does not bind any unwilling country, but it does offer an incentive to follow the European standard.

Several countries and a few specific schemes have been recognized as having adequate data protection, albeit at a slow pace.[151] Other countries amended their laws towards the EU's

---

[147] *See* Council Directive 95/46, *supra* note 1, art. 26(1)(a).

[148] *Id*. arts. 26(2), (4). This avenue has been under-used. *See Commission Staff Working Document on the Implementation of the Commission Decisions on Standard Contractual Clauses for the Transfer of Personal Data to Third Countries (2001/497/EC and 2002/16/EC)*, SEC (2006) 95 final (Jan. 20, 2006), http://ec.europa.eu/justice/policies/privacy/docs/modelcontracts/sec_2006_95_en.pdf, on the implementation of the Commission decisions on standard contractual clauses for the transfer of personal data to third countries.

[149] Council Directive 95/46, *supra* note 1, art. 26(2). Over the years, the Article 29 Data Protection Working Party [hereinafter Art. 29 DPWP], has issued explanations and clarifications about this process. See, for example, Art. 29 DPWP, *Working Document: Transfers of Personal Data to Third Countries: Applying Article 26(2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers*, WP 74 (June 3, 2003), *available at* http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2003/wp74_en.pdf (setting guidelines for approval of BCRs); Art. 29 DPWP, *Working Document Establishing a Model Checklist Application for Approval of Binding Corporate Rules*, WP 108 (Apr. 14, 2005), *available at* http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2005/wp108_en.pdf (evaluating the process, finding it to be long, cumbersome, and expensive, and suggesting ways to streamline the process). In 2010, the EU Commission updated its decision on the matter, to address the increasing practice of global outsourcing of data processing. *See* Art. 29 DPWP, *Opinion 3/2009 on the Draft Commission Decision on Standard Contractual Clauses for the Transfer of Personal Data to Processors Established in Third Countries, Under Directive 95/46/EC (data controller to data processor)*, WP 161 (Mar. 5, 2009), *available at* http://ec.europa.eu/ justice/policies/privacy/docs/wpdocs/2009/wp161_en.pdf .

[150] Art. 29 DPWP, *Party Transfers of Personal Data to Third Countries: Applying Articles 25 and 26 of the EU Data Protection Directive*, WP 12, at 5 (July 24,1998), http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/1998/wp12_en.pdf.

[151] These include *inter alia* Switzerland (recognized in 1999), Argentina (recognized in 2002), Canada (recognized in 2002), Israel (recognized in 2010), Uruguay (recognized in 2010) and a handful of small island nations. For the full list, see *Commission Decisions on the Adequacy of the Protection of Personal*

standards, including Australia, South Africa, India, Turkey, Japan and several South American countries.[152] The overall result is a mechanism of *soft legal globalization*: the law is spread around the globe but not in a hard, binding manner.

The Directive's effect in the United States is more subtle. Thus far, two American schemes earned the European "adequacy" status. The first was the EU-U.S. Safe Harbor program, which created a voluntary framework for American corporations to declare that they adhere to the EU's data protection standards, a statement that is then subject to the FTC's power to investigate and regulate deceptive presentations.[153] Thus, a segment of leading American corporations, including Facebook, Google, LinkedIn, Microsoft and Yahoo! committed to follow European rules.[154] A second scheme was more specific, regarding the transfer of Passenger Name Records (PNR) from the EU to the U.S. as part of anti-terror measures.[155]

Kenneth Bamberger and Deirdre Mulligan studied American privacy practices and discussed the growing attention to data protection issues in corporate America.[156] They found that despite the common view that the American privacy law on the books is inadequate, especially when compared to the European model, the law "on the ground" does provide privacy protection. They argue that in the United States, informational privacy has

---

Data in Third Countries, EUROPEAN COMM'N – JUSTICE, http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm (last updated Oct. 4, 2012). In 2011, a recommendation to declare New Zealand's law adequate was advanced by the Article 29 DPWP. *See* Art. 29 DPWP, *Opinion 11/2011 on the Level of Protection of Personal Data in New Zealand*, WP 182 (Apr. 4, 2011), http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp182_en.pdf.

[152] *See* Birnhack, *supra* note 10, at 515-17; Graham Greenleaf, *83 Data Privacy Laws World Wide*, *in* PRIVACY LAWS & BUSINESS – SPECIAL REPORT (2011).

[153] *See Introduction to the U.S.-EU & U.S.-Swiss Safe Harbor Frameworks*, NAT'L EXPORT INITIATIVE, http://www.export.gov/safeharbor/ (last updated Apr. 11, 2012).

[154] As of February 10, 2012, the number of companies that adhered to the program is 3108. *U.S.-EU Safe Harbor List,* NAT'L EXPORT INITIATIVE, http://safeharbor.export.gov/list.aspx (last visited Jan. 9, 2013) (providing a list of companies that follow the framework).

[155] The negotiations between the U.S. and the EU took several years, with interim setbacks: in 2006 the European Court of Justice annulled the European Commission's decision to recognize the agreement between the U.S. and the EU as adequate. *See* Case C-317/04, Parliament v. Council, 2006 E.C.R. I-4721; Case C-318/04 Parliament v. Comm'n, 2005 E.C.R. I-2467. A new agreement was then negotiated. *See* Council Decision (EC) 2007/551/CFSP/JHA of 23 July 2007, O.J. (L 204) 16.

[156] Kenneth A. Bamberger & Deirdre K. Mulligan, *Privacy on the Books and on the Ground*, 63 STAN. L. REV. 247 (2011).

increasingly received more attention over 15 years (1994-2009). They attribute this growth to the role that the FTC undertook as a regulator of privacy; to the influence of privacy advocates, market and media pressures; and to the new profession of privacy officers.[157] Bamberger and Mulligan identified several indirect European influences on American privacy in practice. One is the Safe Harbor Program.[158] A second point of influence is directly on corporations conducting business with Europe.[159] A third is the interest in smoothing interactions with European regulators, cited as one of the reasons for creating Chief Privacy Officer (CPO) positions in American firms.[160] A fourth instance of European influence occurs when companies draft their global policies.[161] The European standards, as they quote one of their interviewees, are the "highest common denominator."[162] Thus, the EU data protection scheme has not only had a direct effect on other countries' laws, but also an indirect effect, by setting *de facto* commercial standards, on a global scale.

To date, the Directive still reigns over all other global-scale regulatory approaches to data protection. Its mechanisms and power lie first in that it is *hard law* within the EU, binding its 27 Member States (and also the three members of the European Economic Market), and second, in that it is *soft law* outside the EU, with direct and indirect influence on a growing number of other countries. At least for the time being, the Directive is the most influential data protection legislation on a global scale. Hence it will serve as the main case study and be subjected to "reverse engineering" in the next Part.

4. New Initiatives and Proposals

In recent years there have been new suggestions towards a global data protection regime, but thus far, they have not gained significant power. The Asian Pacific Economic Cooperation (APEC) offered a Privacy Framework in 2004 based on the principle of accountability of data controllers to data subjects;[163]

---

[157] *Id.* at 253.
[158] *Id*. at 262, 266, 285, 312.
[159] *Id*. at 265.
[160] *Id*. at 261-62.
[161] *Id*. at 269-70.
[162] *Id*. at 270.
[163] The principle of accountability appeared in the 1980 OECD Guidelines and has reemerged also in the EU. The Art. 29 DPWP proposed a concrete amendment to the Directive to include a principle of accountability that "would require data controllers to put in place appropriate and effective measures to ensure that the principles and obligations set out in the Directive are complied with and to demonstrate so to supervisory authorities upon request." *See* Art. 29

the OECD attempted to re-enter the data protection world in 2007 with a recommendation on international cooperation in enforcing privacy laws;[164] and in 2009, the International Conference of Data Protection Commissioners adopted the Madrid Declaration on *Global Privacy Standards for a Global World*.[165] While these suggestions received some attention by receiving EU support, they have yet to materialize into actual legal frameworks.

Within the EU, there are discussions towards amending the 1995 Directive. In January 2012, the EU Commission published a comprehensive proposal to enact a European Regulation on data protection to replace the 1995 Data Protection Directive.[166] While a Directive obliges the Member States to enact national laws that apply the Directive's principles, a Regulation is directly applicable. Thus, if adopted, the Regulation would achieve substantial harmonization within the EU. The proposed amendments repeat most of the Directive's rules, but boost the rights of the data subjects, expand the duties imposed on the data controllers and processors, provide more and better enforcement tools, and suggest various organizational and governmental mechanisms. The legislative process is likely to take a few years. I will refer to it inasmuch as it implicates the issues discussed here.

The proposals are to adopt new substantive principles, especially the principles of *transparency* and *accountability*, which would require data controllers to be more transparent about their data-related activities, so as to enable better enforcement of the duties imposed on data controllers.[167] A second proposed principle which deserves much attention in the data protection world these days is that of *Privacy-by-Design* (PbD) (renamed data protection by design.)[168] A third principle is the so-called "right to be

---

DPWP, *Opinion 3/2010 on the Principle of Accountability*, WP 173, at 2 (July 13, 2010); OECD GUIDELINES, *supra* note 101. Thus, the principle is seen as a means to promote enforcement.

[164] *See* ORG. FOR ECON. COOPERATION AND DEV. (OECD), RECOMMENDATION ON CROSS-BORDER CO-OPERATION IN THE ENFORCEMENT OF LAWS PROTECTING PRIVACY (2007), *available at* http://www.oecd.org/internet/interneteconomy/38770483.pdf.

[165] *See* Global Privacy Standards for a Global World, *Madrid Privacy Declaration*, THE PUBLIC VOICE (Nov. 3, 2009), http://thepublicvoice.org/TheMadridPrivacyDeclaration.pdf.

[166] *See Proposed GDP Regulation*, *supra* note 6.

[167] *See id.* arts. 5(a) (general principles of personal data processing), 11 (transparent communication to the data subject), 22 (responsibilities of the data controller).

[168] *See id.* art. 23. In 2010, the annual International Conference of Data Protection and Privacy Commissioners adopted PbD as its recommendation. *See Resolution on Privacy by Design*, 32ND INT'L CONFERENCE OF DATA PROT. AND PRIVACY COMM'RS (Oct. 27-29, 2010), http://www.justice.gov.il/NR/

forgotten," which is the right to object to further processing of personal data or to require that the data be deleted.[169] The Commission suggested yet another principle, of *data portability*, which would mean that users would be able to transfer their own data from one service provider to another, e.g., from one social network to another.[170]

The European bodies explain the need to review the Directive in terms of the need to meet challenges of globalization and new technologies.[171] However, many of the proposals are driven by internal EU changes and its perceived need for internal harmonization, as well as an interest in improving enforcement and dealing with new business models that challenge existing rules, such as the outsourcing of data processing to non-EU countries.

Thus, the EU Directive is currently a global leader in data protection. It is a complex set of rules that are structured around the idea of FIPs. At present, the Directive has been the most influential legal instrument in the world of data protection. It is currently at an important junction, with concrete proposals to amend it. Hence, it serves as the subject of *reverse engineering the law*.

V. REVERSE ENGINEERING THE DATA PROTECTION DIRECTIVE

The European Commission and its professional arm, the Article 29 Working Party (somewhat unimaginatively named after Article 29 of the Directive), have announced more than once their view that the Data Protection Directive is technology-neutral. This Part scrutinizes these statements. Section A begins with a

---

rdonlyres/F8A79347-170C-4EEF-A0AD-155554558A5F/26502/ResolutiononPrivacybyDesign.pdf.

[169] *Proposed GDP Regulation*, *supra* note 6, art. 17. *See also* VICTOR MEYER-SCHÖNBERGER, DELETE – THE VIRTUES OF FORGETTING IN THE DIGITAL AGE (2009).

[170] *Proposed GDP Regulation*, *supra* note 6, art. 18. Presumably, such a principle would, for example, require Facebook to enable users to export their data to Google Plus. The Commission provided social networks as an example, in the opening comments of the Proposed GDP Regulation. *Id.* recital 55.

[171] *See id.* recital 5 ("Rapid technological developments and globalisation have brought new challenges for the protection of personal data. The scale of data sharing and collecting has increased spectacularly. Technology allows both private companies and public authorities to make use of personal data on an unprecedented scale in order to pursue their activities. Individuals increasingly make personal information available publicly and globally. Technology has transformed both the economy and social life, and requires to further facilitate the free flow of data within the Union and the transfer to third countries and international organisations, while ensuring a high level of the protection of personal data.").

discussion of the EU perspective on the relationship between technology and data protection law, a perspective that cherishes technology-neutral legislation. I then explain this perspective in the terms presented in Part III (technology-neutral/technology-specific legislative technique). Section B offers a reading of some of the legal and conceptual building blocks of the Directive. I advance the argument that the Directive is better understood as "technology-based but viewpoint-neutral," in that it assumes a specific technological environment, though on a rather abstract level. Along the way, I shall refer to the proposed EU Regulation, which the EU currently discusses as a replacement for the Directive, where relevant.

A. The Directive and Technology

The European Union firmly believes that its data protection law is technology-neutral. The various European bodies that administer the Directive are well aware of its complex relationship with technology. A 2003 Review of the Directive stated that "[d]espite the doubts raised during the negotiation of the Directive, Member States have thus reached the conclusion that the Directive's ambition to be technology-neutral is achieved, at least as regards the processing of sound and image data."[172] A 2009 report of the Article 29 Working Party concluded that "Directive 95/46/EC has stood well the influx of these technological developments because it holds principles and uses concepts that are not only sound but also technologically neutral. Such principles and concepts remain equally relevant, valid and applicable in today's networked world."[173] A 2010 Communication of the European Commission commented that "[t]he findings [of the EU's review of the current legal framework] confirmed that the core principles of the Directive are still valid and that its technologically neutral character should be preserved. However, several issues were identified as being problematic and posing specific challenges."[174] External observers also pointed to the

[172] *See* Comm'n of the European Communities, *First Report on the Implementation of the Data Protection Directive (95/46/EC)*, at 20, COM (2003) 265 final (May 15, 2003) [hereinafter 2003 Review].

[173] *See* Art. 29 DPWP & Working Party on Police and Justice, *The Future of Privacy - Joint Contribution to the Consultation of the European Commission on the Legal Framework for the Fundamental Right to Protection of Personal Data*, WP 168, at 3 (2009) [hereinafter WP 168].

[174] *See Communication from the Commission to the European Parliament, The Council, The Economic and Social Committee and the Committee of the Regions - A Comprehensive Approach on Personal Data Protection in the European*

technology-neutral position of the Directive as one of its strengths.[175]

The European Union believes that the principled neutrality has enabled the Directive to remain valid almost two decades after it was first discussed. The following passage from a 2009 report of the Article 29 Working Party is telling:

> The basic concepts of Directive 95/46/EC were developed in the nineteen seventies, when information processing was characterized by card index boxes, punch cards and mainframe computers. Today computing is ubiquitous, global and networked. Information technology devices are increasingly: miniaturized and equipped with network cards, WiFi or other radio interfaces. In almost all offices and family homes users can globally communicate via the Internet. Web 2.0 services and cloud computing are blurring the distinction between data controllers, processors and data subjects.
>
> Directive 95/46/EC has stood well the influx of these technological developments because it holds principles and uses concepts that are not only sound but also technologically neutral. Such principles and concepts remain equally relevant, valid and applicable in today's networked world.[176]

Thus, the data protection regulators believe the Directive is technology-neutral and emphasize its flexibility. Their conclusion is that the Directive does require some amendments,[177] but none are radical, in terms of the fundamental principles or the assumption as to the underlying technologies. Moreover, the EU Commission believes neutrality is crucial. In its proposed Regulation, it states that "[t]he protection of individuals should be technologically neutral and not depend on the techniques used; otherwise this would create a serious risk of circumvention."[178] The example provided in the proposed Regulation is about manual processing, which should also be subject to the Regulation, if the

---

Union, at 3, COM (2010) 609 final (Nov. 4, 2010) [hereinafter COM (2010) 609].

[175] *See*, *e.g.*, NEIL ROBINSON, ET AL., REVIEW OF THE EUROPEAN DATA PROTECTION DIRECTIVE 24 (2009); *id.* at 22 (attributing the Directive's sustainability to its principle-based framework).

[176] WP 168, *supra* note 173, ¶¶ 41-42.

[177] *See* COM (2010) 609, *supra* note 174, at 18; WP 168, *supra* note 173.

[178] *See Proposed GDP Regulation*, *supra* note 6, recital 13.

processing aims to create a database ("filing system").[179]

The Directive's key constructs are all phrased in general language. These building blocks include the definitions of personal data, data controller, and processor as well as a structure of according some rights to data subjects, imposing duties on the controllers, and creating dual private and regulatory enforcement mechanisms. The Directive does not speak of any particular technological method of collecting or processing data. The choice of a technology-neutral legislative technique surely has made a substantial contribution to the Directive's sustainability, though there are probably additional factors that made the Directive resilient to technological changes.[180]

The Directive's technology-related choices fit the considerations mentioned earlier, especially those of flexibility and harmonization. The need for flexibility is obvious, and the founders of the Directive are aware of it. Harmonization is crucial once we take into consideration the European political map. The Directive is a general piece of legislation directed at the Member States of the EU, rather than at local courts. To achieve harmonization among the Member States, a much sought-after goal of the EU, the Directive could choose a rather abstract language, or alternatively, it could be replaced with a directly applicable Regulation. The political form of the Directive further means that the national legislatures and regulators enjoy a margin of appreciation, to use European parlance, meaning that they have the permission and leeway to take more concrete stances, as long as they are in line with the Directive. Interestingly, the European discourse on data protection goes beyond harmonization within the EU and in recent years has included discussion of the global dimension. As for consideration of innovation, thus far this has not been part of the European discourse on the Directive's technological neutrality. The proposed Regulation mentions innovation in an almost inadvertent manner.[181]

---

[179] *Id*.

[180] An important factor that explains the Directive's continuing relevance and power is its combination of being mandatory within the EU and its sophisticated export mechanism in the form of what I call *soft legal globalization*. The weakness of the national and international alternatives (the OECD Guidelines, the CoE Convention, the UN Guidelines, the APEC Framework, and the data commissioners' declarations) provide yet another explanation for the Directive's resilience.

[181] In the explanatory note, the Proposed GDP Regulation mentions that lack of trust in the online environment "risks slowing down the development of innovative uses of new technologies." *Proposed GDP Regulation*, *supra* note 6, at 1. In the context of data security rules, the proposal states that "the

But what sort of technology neutrality does the EU apply? Phrased in the typology offered earlier, we can characterize it as the following: *first*, on the end-means continuum, the subject matter of the Directive is data protection. Unlike patent law or e-commerce legislation, the Directive is not meant to regulate technology directly. Neither is technology perceived as a means to achieve the goal (subject to the exception of Privacy Enhancing Technologies (PETs) and Privacy by Design (PbD)). Instead, the Directive treats technology as a given fact, acknowledging that various technologies affect the possibilities and practices of data collection, processing and transfer. Accordingly, as far as personal data is regulated directly, technology is taken for granted, as if it were a closed "black box": the Commission does not know what is inside the box and hence defines its content in general terms – namely, technology-neutral terms. Nevertheless, as I will show later, there are some hidden assumptions as to the contents of this box.

Second, on the promotion-restriction continuum, the Directive is placed in a safe place in the middle: it passively permits new technologies. The Directive does not actively promote new technologies, nor does it restrict them. In fact, the Directive does not say anything about the technologies themselves. It sets its principles as to what human (as well as corporate and perhaps governmental) players can or cannot do with the technologies. The duties and rights are all based on general principles (which are concretizations of the overarching principle of fairness and lawfulness) and on general functions (e.g., the purpose limitation principle).

Third, on the abstraction-concretization continuum, the Directive seems to have chosen a rather abstract position. No specific technologies are mentioned. The Directive opted for a technology-neutral language. However, as I shall argue in the next section, the Directive is less neutral than this first impression would suggest.

The proposed Regulation also focuses on data protection. It states that the new technologies are the trigger for the proposal, but in the same breath, the proposal explicitly adheres to the principle of technology neutrality. The proposed Regulation does cite several specific technologies: it mentions the Internet and tracking technologies,[182] and more specifically, "online identifiers," such as

Commission should promote technological neutrality, interoperability and innovation." *Id.* recital 66.

[182] *Proposed GDP Regulation*, *supra* note 6, recital 21.

Internet Protocol addresses and cookies.[183] The Internet is also a prime example in the case of the right to be forgotten,[184] and in the discussion of some business models, such as online advertising.[185] Social networks are provided as an example for the need for data portability; namely, the subject's right to switch from one social network to another with his or her data.[186] Another important principle embraced by the proposal is that of PbD: data controllers will be required to implement such measures.[187] The PbD principle does not dictate a particular technology to be used, but it does assume that technology is embedded with social values and thus that it is regulable.

B. The Directive and Technology Neutrality

Reverse engineering the Data Protection Directive questions whether or not the Directive is actually technology-neutral. The skepticism which I apply here is instrumental, meant to serve as a tool to expose the technological mindset within which the Directive was drafted and within which it operates.

The Directive does use technology-neutral language. Its only direct explicit reference to technology is in Article 33, where it instructed the Commission to examine the Directive's application "to data processing of sound and image data," and submit proposals that would take into account "development in information technology."[188] Later on, the Commission reached the conclusion that the Directive does cover sound and image data.[189]

In this sense the Directive is technology-neutral and can encompass health-related data, financial data, and genetic data, collected or processed in, for example, a computer, network or biometric manner. But, a closer view reveals that the Directive assumes a general structure about personal data: what is its nature and what happens to it. More specifically, the Directive assumes a linear life cycle of personal data. It assumes a sequence of

---

[183] *Id.* at recital 24.
[184] *See id.* at recital 53.
[185] *See id.* at recital 46.
[186] *See id.* at recital 55.
[187] *See id.* at art. 23, recital 61.
[188] *See* Council Directive 95/46, *supra* note 1, at art. 33.
[189] *See* 2003 Review, *supra* note 172, § 5, at 20; *see also* Article 29 DPWP, *Opinion 4/2007 on the concept of personal data*, WP 136, at 7 (June 20, 2007) [hereinafter WP 136] (concluding that sound and image data qualify as "personal data"). For a discussion of sound and image data under the Directive, see Jacqueline D. Lipton, *Digital Multi-Media and the Limits of Privacy Law*, 42 CASE W. RES. J. INT'L L. 551 (2010), which argues that existing privacy law, including the Directive, focuses on text-based personal records.

collection, processing and transfer of personal data, all of which take place between two parties. This is a technological assumption, as it is based on the technologies that were available in the 1970s and still persist. But new technologies might change the sequence. A second technological assumption is that the personal data has a destination: to be part of a database. The idea of a database is a formative one in the Directive's structure.

The Directive and its entire data protection regime operate within this technological paradigm. It is broad enough and still valid to a large extent so as to capture both the form of data processing of the 1970s and of the early 2010s, but we are beginning to see its limits. From this point of view, we are not yet experiencing a technological paradigm shift, but there are signs that such a shift is likely to occur in the not too distant future.

To make the case, I discuss the definitions of personal data, processing of personal data, and personal data filing systems. Along the discussion we will also meet the players whom the Directive envisions: the data subject, the data controller, and the data recipient. Together, these form the building blocks of the Directive and its legal structure.

1. Personal Data

The fundamental construct of the entire data protection legal regime is its definition of *personal data*, which is bundled with the definition of data subject: "any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity . . . ."[190]

There are many interpretive questions about the scope of the definition and some of its elements.[191] Here I focus on the definition's technological assumption. The criterion applied by the

[190] Council Directive 95/46, *supra* note 1, at 38, art. 2(a). The Proposed GDP Regulation separates the two definitions, defining "personal data" to mean "any information relating to a data subject," (see *Proposed GDP Regulation*, *supra* note 6, at art. 4(2)) and "data subject" to mean "an identified natural person or a natural person who can be identified, directly or indirectly, by means reasonably likely to be used by the controller or by any other natural or legal person, in particular by reference to an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person" (see *Proposed GDP Regulation*, *supra* note 6, at art. 4(1)). The definition of data subject adds technological references of location data, online identifier and genetic identity.

[191] *See* WP 136, *supra* note 189.

Directive to identify *personal* data is the identification of the subject rather than the content of the data. Unlike the American sectoral approach, which points to specific kinds of data (plus governmental data and data about children under the age of thirteen), the Directive is at first blush agnostic regarding the content. The Directive does treat some data as more sensitive than others and requires additional legal attention to "special categories of data," which are defined as "data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life."[192] But this layer of content-based personal data is a second layer, on top of the identification-based layer.

Perhaps the American sectoral approach might match common wisdom more directly: most of us would agree that certain kinds of data are more sensitive than others. Such a consensus might change over time and differ from place to place, reflecting local culture and perhaps history. The European approach, in its choice of identification as the basic criterion for its regulatory scheme, departs from such an imagined common wisdom. Importantly, the American approach does not end with the content-based criterion: most of the federal informational privacy laws apply the European standard of identification. Most contemporary laws that regulate personal data are triggered if the data collected and processed is personally identifiable information (PII).[193]

However, viewed on the background of digital technology, the European approach reflects a digital mindset, whereas the content-based approach reflects an analogue one. The digital mindset acknowledges that seemingly innocent pieces of data can be combined to form a whole that is greater than the sum of its parts. While aggregating data and analyzing it is a technologically-neutral activity, digital technologies enable the aggregation of mass quantities of data--their constant updating and, most importantly, mining the data, in a way that is different in kind, not only in quantity, than the equivalent analogue activities. To be subject to digital mining, the data need not be structured in any

[192] Council Directive 95/46, *supra* note 1, at 40, art. 8(1). The Proposed GDP Regulation adds reference to the processing of genetic data and criminal convictions or related security measures. *See Proposed GDP Regulation*, *supra* note 6, at art. 9(1).

[193] *See* Paul M. Schwartz & Daniel J. Solove, *The PII Problem: Privacy and a New Concept of Personally Identifiable Information*, 86 N.Y.U. L. REV. 1814 (2011).

way, unlike analogue databases and their analysis.[194] The facts of one's name, date of birth, religion, ethnicity, gender, sexual orientation, profession, social relationship, personal status, financial status, health status, as well as one's online activities, intellectual interests or consumer habits—each on their own might not be considered private by some. More likely, some of us will be more passionate about the privacy of some of these data than of other details. But the combination of some of these details is what matters. Joining together one's religion with one's financial status creates an image, shallow as it might be; joining three facts from the above list, which is by far not an exhaustive one, makes the image more complex, until the accumulation of the data creates our profile. This is not the place to explicate the privacy-related concerns that arise when another person (or government or corporation) holds what it thinks is our profile,[195] or in Daniel Solove's term, our "digital dossier."[196] The point is that the profile is created by joining together bits of information, which are then further analyzed. This is a digital mindset to personal data, in that it is interested in all kinds of data, not only in data that is considered sensitive.

The Directive's approach is thus more advanced than previous approaches, in that it understands the power of joining separate bits together. In its language and references, it is a technology-neutral (and also context-neutral) definition, but it is informed by a digital concept and should be understood within a digital paradigm. For the time being, this is indeed the technological paradigm that we encounter in our daily lives. Note that this is not a historical argument; rather, it is a discursive one. Whether the drafters of the Directive foresaw the digital environment—or whether their reasoning for choosing the identification-based definition was to avoid the difficulty of reaching an agreement on which kinds of data are worthy of legal protection or not—are matters for legal historians to explore. The point is that the Directive easily fits a digital mindset.

In a recent important work, Paul Ohm points to a major technological assumption of the Directive and many, if not all

---

[194] The joint effect of these characteristics of data has earned the title "big data." For a discussion of this effect, see Omer Tene & Jules Polonetsky, *Big Data for All: Privacy and User Control in the Age of Analytics*, NW. J. TECH. & INTELL. PROP. (forthcoming 2013).

[195] On profiling, see PROFILING THE EUROPEAN CITIZEN: CROSS-DISCIPLINARY PERSPECTIVES (Mireille Hildebrandt & Serge Gutwirth eds., 2008).

[196] DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE 2 (*2004*).

other informational privacy legislation.[197] Ohm shows that the legislation assumes that anonymization is possible and thus, informational privacy laws often opt for anonymization as a "silver bullet solution."[198] Indeed, this is what lies at the heart of the Directive's definition of personal data. However, based on contemporary research in the field of computer science, Ohm argued that anonymization is largely an obsolete notion: it is possible to de-anonymize data far more easily than lawyers have thus far assumed. Framed in the terms applied here, Ohm exposed a central hidden technological assumption of data protection law: the law's assumption that there are technologies that can achieve irreversible anonymization. Once this tenet collapses, the data protection regime needs to reconfigure itself.[199] The analysis offered here further deconstructs the façade of technology neutrality: the law seems to be technologically-neutral, but Ohm showed that it assumed a technology of a particular capability, which he then showed was a flawed assumption.

Thus, for the time being, the definition of personal data is rooted within a digital technological paradigm, for good or for bad. The good part is that it is more advanced than the previous, analogue, content-based definition; the bad part is that the concept of non-identification is about to collapse, if it has not already done so. As long as we are within a digital technological paradigm, the definition will suffice, with adjustments needed to answer the challenge of de-anonymization. But, once new technologies appear, perhaps rooted in a different technological paradigm, the definition might reach its natural end.

2. Processing of Personal Data

After defining the key construct, the Directive turns to describe the actions taken in relation to personal data. Such actions all come under the heading of "processing personal data, " which is defined as (the numbering was added to facilitate the discussion that follows):

> any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as [1] collection, [2] recording, [3] organization, [4] storage, [5]

[197] Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701 (2010).
[198] *Id.* at 1736.
[199] For a suggestion, see Schwartz & Solove, *supra* note 1933.

> adaptation or alteration, [6] retrieval, [7] consultation, [8] use, [9] disclosure by transmission, [10] dissemination or [11] otherwise making available, [12] alignment or combination, [13] blocking, [14] erasure or [15] destruction. [200]

This definition should be read along the Directive's Article 3, which defines its scope. On the inclusive side, the Directive applies to automatic and manual processing, if it is to be part of a database (Art. 3(1)).[201] On the exclusive side, the Directive does not apply to national security and law enforcement activities (Art. 3(2)); or to personal activity (Art. 3(2)), so that one's personal email Address Book, for example, is not subject to the Directive.[202]

Let us read the definition closely. It begins with a broad, inclusive statement: "any operation or set of operations which is performed upon personal data" and is then accompanied by a list of activities. It is tempting to search and point to a category of processing that is not listed, but the Directive anticipated this, in its broad opening definition and in that the list is only illustrative ("such as"). Legally, the definition will cover new situations quite easily: either they would fall within a specific example or they are within the more general "use," which seems to be the most open-ended illustration.

Such an expansive function-based definition is indeed technology-neutral. We can test this neutrality by considering several technologies that emerged after the Directive was adopted. For example, RFID tags can collect, record and store data; they enable the data's retrieval, use, and disclosure.[203] Geo-location

---

[200] Council Directive 95/46, *supra* note 1, at 38, art. 2(b). Compare it to the taxonomy offered by Daniel Solove, which is divided into four clusters: collection, processing, dissemination and invasion. Each cluster is then sub-divided into further kinds of activities. *See* DANIEL J. SOLOVE, UNDERSTANDING PRIVACY 103 (2008). The *Proposed GDP Regulation*, *supra* note 6, at art. 4(3), adds to this list "structuring" as the fourth situation in the list and deletes "blocking."

[201] Council Directive 95/46, *supra* note 1, at 39, art. 3(1) reads: "This Directive shall apply to the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system." The *Proposed GDP Regulation* maintains the same definition, with minor stylistic changes. *See supra* note 6, at art. 2(1).

[202] The *Proposed GDP Regulation* maintains these exclusions. *See id*. art. 2(2).

[203] The Art. 29 Data Protection Working Party considered the matter and responded in the affirmative. Art. 29 DPWP, *Working Document on Data Protection Issues Related to RFID Technology*, WP 105 (Jan. 19, 2005), *available at* http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2005/wp105_en.pdf.

technologies such as GPS enable the collection of one's location, recording, organizing, and storing the data, so that it is adaptable, retrievable, used, disclosed, disseminated, made available to others, blocked, or erased.[204]

But the reading offered here is interested not only in the legal scope, in which the Directive fares well, but in its underlying technological assumptions. Hence, we should read the list in a different way. The illustrative list is organized in a particular manner. It is quite apparent that the organizing theme is a chronological sequence. I classify the components into several clusters: input, management, internal usage, external usage (or output) and clean-up.

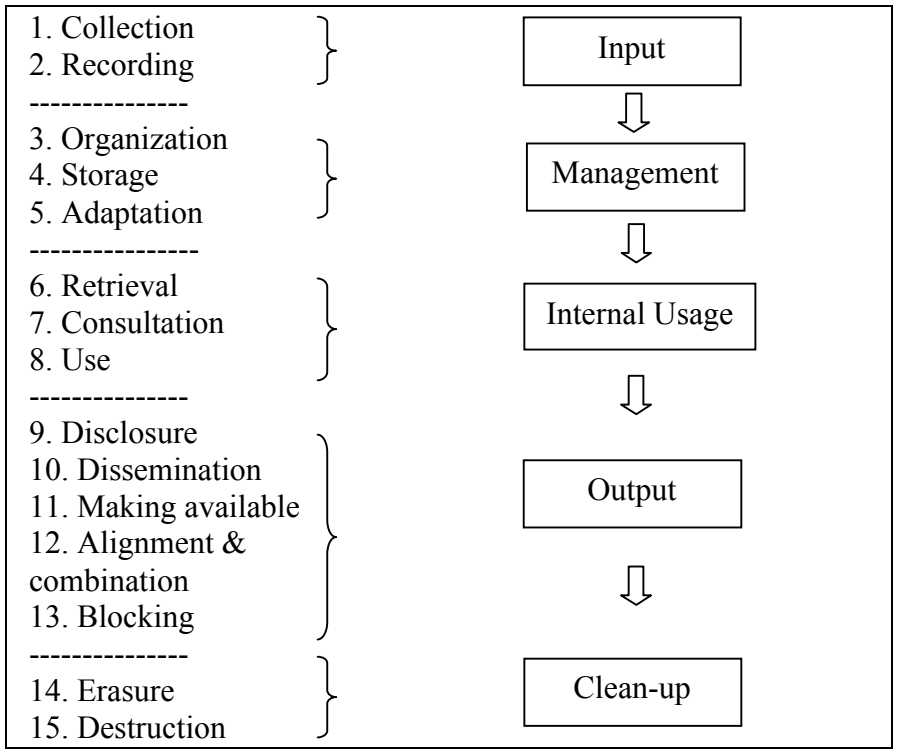
Accordingly [see figure 1], steps 1-2 (collection, recording) describe *input*; steps 3-5 (organization, storage, adaptation) refer to the *management* of the database; steps 6-8 (retrieval, consultation, use) are *internal usage*; steps 9-12 (disclosure, dissemination, making available, alignment or combination) are *output*.[205] Step 13 (blocking) probably refers to external access to the data and if so, it is an aspect of *output*.[206] The last two steps (erasure and destruction) are post-mortem *clean-up*: what happens with the data once it is no longer in use.

[204] Once again the Art. 29 Data Protection Working Party considered the matter and took it for granted that data collected about an identified person by geo-location technologies is "processing." *See* Art. 29 DPWP, Opinion 13/2011 on Geolocation Services on Smart Mobile Devices, WP 185 (May 16, 2011), *available at* http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp185_en.pdf.

[205] Step 12, alignment or combination, can also be classified as usage (though in an external manner) by matching separate databases, once again reflecting the digital state of mind under which the combination of innocent data is greater than the sum of its parts.

[206] The Proposed GDP Regulation omits "blocking" from the list. *Proposed GDP Regulation*, *supra* note 6, at 41.

Figure 1: The Directive's Linear vision of Data Processing



This reading indicates that the Directive reflects a progressive assumption about personal data. It assumes that data behaves similarly to human beings: it is born, grows up, becomes productive, and ultimately, it dies. Phrased in the human metaphor, the personal data's "home" is the database. There is a further, deeper assumption here. It is that there are preparatory stages that serve as the basis of the real thing: the internal and external usage (output) that lie at the heart of "processing." The first steps (input) are seen as an instrumental part, and the final steps (clean up) are seen as a wrapping up mechanism. The focus is on the central activities; those of processing.

Thus read, the sequence of the illustrative list assumes a temporal linearity. It is a sensible and plausible approach. In fact, it is difficult to think of any other coherent way to organize the possible activities regarding personal data, unless we give up such an attempt altogether, or perhaps search instead for a functional definition ("all activities"), or one that is based on a delegation of power ("whatever the data subject consents to/disagrees with"). But, once again, the linear sequence assumes a particular technological environment. The linearity assumes that first data is

collected, then stored in a database, and only then is it used and might also be transferred to third parties.[207]

The linearity further assumes that there are a few players involved; each appears in a different segment of the structure [see figure 2]. The Directive casts a few such players: data subject,[208] data controller,[209] data processor,[210] a third party,[211] and a recipient.[212] The players in the initial input steps are the data subject and the collector, which is considered by the Directive to be the controller; the chief player in the steps of management and internal usage is the data controller, perhaps with the assistance of the data processor; the players in the output steps are the data controller and the recipient of the data. The final steps (clean-up) are in the hands of the data controller.

[207] Lipton argues that many legislatures were concerned more with the collection of personal data, but that in recent years legislatures treat collection and dissemination on a continuum. Her example of the newer approach is the EU Directive. *See* Lipton, *supra* note 189, at 552.

[208] As noted earlier, the data subject is defined in the Directive's definition of personal data as "an identified or identifiable natural person." Council Directive 95/46, *supra* note 1, at art. 2(a).

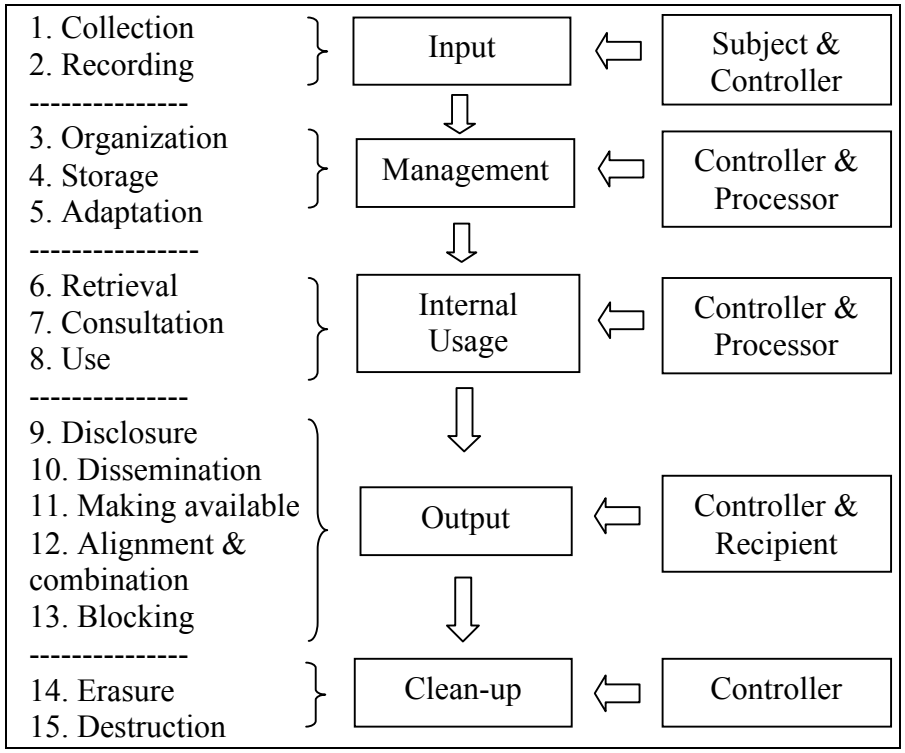
[209] A data controller is defined in the Directive as "the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data." Council Directive 95/46, *supra* note 1, at art. 2(d). The *Proposed GDP Regulation*, *supra* note 6, at art. 4(5) adds "conditions" between the "purposes" and "means."

[210] A data processor is defined in the Directive as "a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller." Council Directive 95/46, *supra* note 1, at art. 2(e). The *Proposed GDP Regulation*, *supra* note 6, at art. 4(6) maintains this definition.

[211] A third party is defined in the Directive as "any natural or legal person, public authority, agency or any other body other than the data subject, the controller, the processor and the persons who, under the direct authority of the controller or the processor, are authorized to process the data." Council Directive 95/46, *supra* note 1, at art. 2(f). The *Proposed GDP Regulation*, *supra* note 6, omits this definition.

[212] A recipient is defined in the Directive as "a natural or legal person, public authority, agency or any other body to whom data are disclosed, whether a third party or not" and excludes authorized authorities. Council Directive 95/46, *supra* note 1, at art. 2(g). The *Proposed GDP Regulation*, *supra* note 6, art. 4(7) omits the reference to a third party and the exclusion of authorities.

Figure 2: The Players



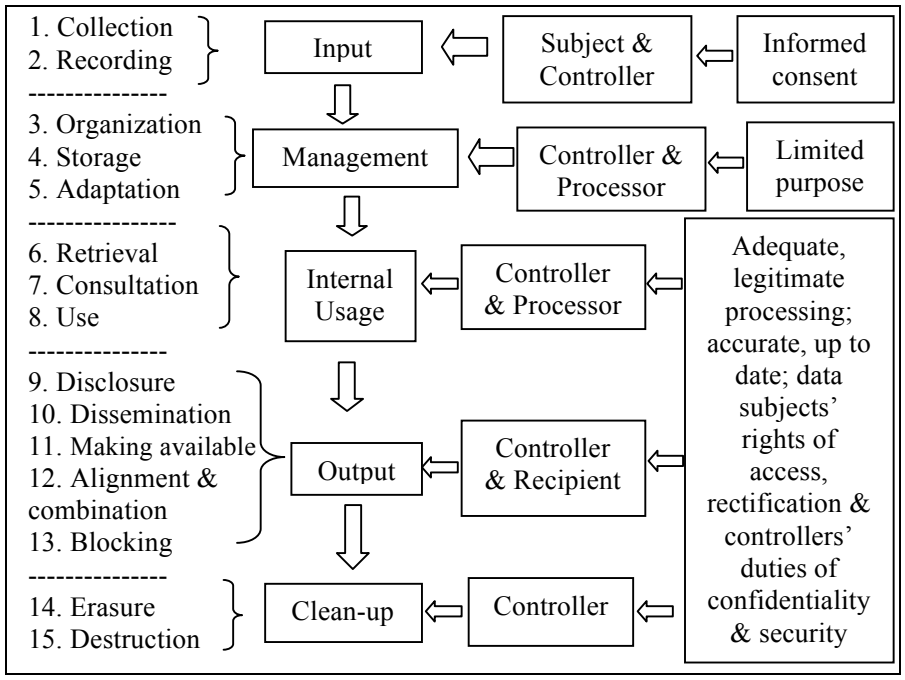
The assumption about linearity, the segmentation, and the casting of different players to each segment create several meeting points between the segments and between the players in charge. The first meeting point, in the first segment (input), is between the source of the data (usually the data subject, but it can also be other sources)[213] and the data controller (either the collector or the processor on the controller's behalf). The second and third segments (management and internal use) are under the direction of the data controller, alone or with the assistance of a data processor. The fourth segment (output) sees the meeting point of the controller and a recipient. The final segment (clean-up) is once again under the direction of the controller (or the processor, on the controller's behalf).

The graphic depiction reveals one of the most acute challenges with which the Directive strives to deal: the data subject has a role only in the first stage. How, then, can the data subject extend his or her control over the later segments, where the subject is no longer part of the picture? Due to the subject's disappearance

[213] Art. 11 addresses the situation where the data have not been obtained from the data subject. Council Directive 95/46, *supra* note 1, at art. 11.

from later stages, the first meeting point becomes especially crucial. If the source of the data is the data subject herself, it is the time and place where the collector can convey information to the data subject and the data subject can exercise control: that is the point when she can consent (or decline). Accordingly, the data subject should be informed, either if the data is collected directly from her (Art. 10) or if it is collected from another source (Art. 11); the purpose of the collection should be specified and explicit and the data can be used only in a way that is compatible with that purpose (Art. 6(1)(b)). Moreover, the data can be processed only upon the unambiguous consent of the data subject (Art. 7(a)), with some listed exceptions (Art. 7(b-f)). The Directive enables the data subject some power to assure her rights are not violated, by way of the rights of access and rectification (Art. 12). But the Directive acknowledges that these rights are insufficient and hence subjects the controllers to further duties. Above all, processing should be fair and lawful (Art. 6(1)(a)), and specifically, it should be for a legitimate purpose (Art. 6(1)(b)); the data collected should be adequate, relevant, and not excessive in relation to the purposes for which they are collected (Art. 6(1)(c)); the personal data collected should be accurate and, where necessary, kept up to date (Art. 6(1)(d)); and kept in a form which permits identification of data subjects for no longer than is necessary (Art. 6(1)(e)). Moreover, the data controller should maintain confidentiality and security (Art. 16, 17). The mechanisms are meant to extend the data subject's control beyond the first stage [see figure 3].

Figure 3: Data Subjects' Rights



The aggregate result is that the Directive provides a legal toolkit that creates rights for the data subject, effectively extending the subject's control beyond the first stage.[214] In practice, there are many difficulties with this structure: the rights are not always respected, the duties are not always fulfilled, and enforcement does not always succeed. The proposed principle of accountability might help in providing data subjects and regulators with more tools to address this challenge.[215] These issues do require attention. However, for the purposes of the mission undertaken here, we can assume that the legal structure does work. The query is about the hidden technological assumptions.

The linear data collection and processing mindset fits most technologies with which we are familiar today and the business models that utilize these technologies. We provide data to various service providers (schools, banks, doctors, communication providers, websites, vendors, etc.) who then process it in various

[214] The Proposed GDP Regulation seems to have identified the problem of the data subject's limited control and suggests strengthening the power of data subjects in all current meeting points by requiring more transparency on behalf of the data controller and processor. Moreover, the proposal adds new meeting points, notably the right to be forgotten, which would enable users to demand the erasure of their data in certain circumstances. *Proposed GDP Regulation*, *supra* note 6.

[215] For the proposals of a principle of accountability, *see* note 163.

internal and external ways. But future technologies might challenge this linear sequence.

The various ways in which new technologies defy the current technological assumptions and the legal structure that the Directive built upon are yet to be explored. In the meantime, we can note a few clear technological trends that have already been identified, including by the EU itself: *first*, more data is collected in more settings and in less detectable ways.[216] *Second*, a specific technology is the growing use of cloud computing.[217] This means that more kinds of data, including personal data, are no longer stored on the user's hard disk, but elsewhere. The implication is that as far as such cloud-stored data includes personal data, the data subject has even less control over the data.[218] *Third*, data subjects can hardly control some kinds of data about themselves. Examples are genetic, biometric, and cognitive data, and data about our personality, behavior, and, perhaps one day, also our thoughts.[219] In the absence of physical ability to control the data, the law can provide subjects with such control. One commercial application based on such tacit data is already gaining market power: Online Behavioral Advertisement (OBA), i.e., targeted ads based on one's behavior.[220] *Fourth*, new network applications, especially social networks, enable (or perhaps push) users to share personal data. The issue of privacy in social networks deserves much attention,[221] but the intertwined technological and social assumptions of the Directive fail to address much of what is going on in such environments. All the Directive can do is address the relationship between the users and the platform, namely between

[216] 2003 Review, *supra* note 172, § 1.2. Accordingly, the Proposed GDP Regulation emphasizes the importance of explicit consent. *Proposed GDP Regulation*, *supra* note 6, recital 33 and art. 8.

[217] WP 168, *supra* note 174, at 2.

[218] For cloud computing and its implications on data protection, see Robert Gellman, *Privacy in the Clouds: Risks to Privacy and Confidentiality from Cloud Computing*, WORLD PRIVACY FORUM, (Feb. 23, 2009), http://www.worldprivacyforum.org/pdf/WPF_Cloud_Privacy_Report.pdf.

[219] For an analysis of the privacy implications of future technologies, see *Final Horizon Scanning Report*, PRACTIS – PRIVACY APPRAISING CHALLENGES TO TECHNOLOGIES AND ETHICS (July 2011), http://practis.org/docs/PRACTIS% 20D2%202_130711final.pdf.

[220] For a recent discussion, see Omer Tene & Jules Polonetsky, *To Track or "Do Not Track": Advancing Transparency and Individual Control in Online Behavioral Advertising*, 13 MINN. J.L. SCI. & TECH. 281 (2012).

[221] *See*, *e.g.*, Lilian Edwards & Ian Brown, *Data Control and Social Networks: Irreconcilable Ideas?*, *in* HARBORING DATA: INFORMATION SECURITY, LAW AND THE CORPORATION 202 (Andrea M. Matwyshyn ed., 2009); James Grimmelmann, *Saving Facebook*, 94 IOWA L. REV. 1137 (2009).

an end-user and the operator of the social network.[222] However, the technology enables each user to reveal data not only about himself but also about his "friends," including tagging photographs in which they appear and much more.[223] The Directive is simply unequipped to deal with this new source of threat to our privacy.[224]

Thus, more technologies collect data in a way that bypasses the initial meeting point between the subject and the controller, a point envisioned by the Directive and much relied upon. The Directive assumes the subject could exercise control if he or she were to know and be given an opportunity to make an informed decision. Reality has proven that bounded rationality, cognitive failures, limited attention, and low awareness, on occasion in unequal settings (such as employment), mean that the subject cannot exercise meaningful control.[225] But without an initial meeting point in the first stage of the chain of data processing, the Directive's vision of personal data and its processing crumbles and might fall apart.

---

[222] The Art. 29 Data Protection Working Party examined social networks and concluded that providers are data controllers and that most users act for purely personal or household activity, which is exempt from the Directive. The WP clarified the obligations of the operators and the rights of subjects, but could not do more regarding the users' interaction with each other, other than requiring the provider to advise the users that information about others should not be uploaded without the other person's consent. *See* Art. 29 DPWP, *Opinion 5/2009 on Online Social Networking*, WP 163 (2009), *available at* http://ec.europa.eu/ justice/policies/privacy/docs/wpdocs/2009/wp163_en.pdf.

[223] The Art. 29 Data Protection Working Party realized the shortcoming of the Directive in this context. *See* WP 168, *supra* note 173, at 18 (noting that "[h]owever, Directive 95/46/EC does not apply to the individual who uploads the data for 'purely personal' purposes or 'in the course of a household activity'. Arguably it does not apply either to the organization that provides the service, i.e. hosts and makes available the information uploaded by the individual (unless the service processes data for its own purposes) insofar as the service provider may not be deemed to be a controller. The result is a situation of lack of safeguards which may need to be addressed, particularly given the increase in the number of such situations. In this context, whoever offers services to a private individual should be required to provide certain safeguards regarding the security, and as appropriate the confidentiality of the information uploaded by users, regardless of whether their client is a data controller.") (citations omitted).

[224] An empirical study conducted in Israel, which has an EU-adequate data protection legal regime, confirms this argument. *See* Michael D. Birnhack & Niva Elkin-Koren, *Does Law Matter Online? Empirical Evidence on Privacy Law Compliance*, 17 MICH. TELECOM. & TECH. L. REV. 337 (2011).

[225] For a discussion of these failures and some answers, see M. Ryan Calo, *Against Notice Skepticism in Privacy (and Elsewhere)*, 87 NOTRE DAME L. REV. 1027 (2012). The *Proposed GDP Regulation* suggests that in the case of "significant imbalance between the position of the data subject and the controller," consent cannot provide a legal basis for processing. *See Proposed GDP Regulation*, *supra* note 6, at art. 7(4).

3. Personal Data Filing System – aka Database

The third key construct of the Directive is the filing system, which enters the stage after the definitions of personal data and processing of such data. The discussion of the Directive's definition of "processing" indicated that it was geared towards the database. The definition of a "data filing system" confirms this tendency. The Directive reveals its line of thought: the destination of the personal data is to be included in a filing system, or, in the popular term, a database. The definition reads: "'personal data filing system' ('filing system') shall mean any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis . . . ."[226]

Once again, the definition seems at first to be technology-neutral. It does not even use the words computer or electronic and indeed, per the Directive, a database also includes manual lists.[227] The Directive further anticipated the option of decentralized systems, where the data is kept separately in two or more places, either in different jurisdictions or split along a criterion of their content. The broad scope is understandable—if a database would have a narrow definition, it would be easy for data controllers to structure their systems around the definition and thus avoid the duties imposed by the Directive.

Nevertheless, I argue that the Directive does assume a particular technological mindset: it is focused on the idea of a database. This is indicated by the close reading suggested above and is further supported by official statements. The historical concerns that drove much of the early data protection legislation focused on the idea of a database: a place where personal data is accumulated.[228] Recall the first principle of the Ware Report in the

---

[226] Council Directive 95/46, *supra* note 1, at art. 2(c). The *Proposed GDP Regulation*, *supra* note 6, at art. 4(4) maintains this definition.

[227] Council Directive 95/46, *supra* note 1, at art. 3(1). The EU insists on covering manual databases. When it found the data protection laws of some countries to be adequate, even though these laws did not cover manual databases, the adequacy finding excluded the status from such databases. *See*, *e.g.*, Art. 29 DPWP, *Opinion 6/2009 on the Level of Protection of Personal Data in Israel*, WP 165, at 5 (Dec. 1, 2009), *available at* http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp165_en.pdf (finding that "it is not possible to consider the Israeli legislation as adequate with regard to non-automated or manual processing systems.").

[228] *See* William H. Ware, et al., *Preface: Report of the Secretary's Advisory Committee on Automated Personal Data Systems,* U.S. DEP'T OF HEALTH, EDUC. & WELFARE (July 1973), http://epic.org/privacy/hew1973report/ (quoting HEW Secretary Elliot Richardson's findings: "there is a growing concern that

United States in 1973 – there should be no secret databases.[229] In the absence of legal historical research, we can speculate that the reason for the focus on databases was the growing use of computers in the 1970s, especially by the government, and the negative memory of "black lists" that evolved into a database. By the time the European Directive was discussed in the early 1990s, computers were widely used by the private sector. Manual lists evolved into digital dossiers.[230]

The focus on databases and the broad definition capture much of the data processing that takes place today, and that will take place in the near future. But we can already see its limits. One situation in which there is ample use (or processing, to stick to the Directive's definitions) of personal data is in unstructured data, often referred to as Big Data. Technological mining capabilities render the pre-structuring of the data irrelevant. The data is collected but not arranged in any way. It is then mined in a way that produces meta-data: data about the data.[231]

A second situation, which defies the Directive's technological mindset, is the social setting, where users of systems publish, tag and process personal data of other users--put simply, social networks. The problem is that the risk to private data stems not only from the government or the market, but from our peers. Jonathan Zittrain called this *Privacy 2.0*, to denote its sphere in the Web 2.0 environment.[232] The Directive assumes a technological environment of Web 1.0 and the related Privacy 1.0, where there is a powerful player (the data controller). Arguably, we can view a social network collectively as a database, i.e., as a filing system, though we might need to spend some effort in explaining how it is "structured" and how it is "accessible according to specific criteria." Think of Facebook, LinkedIn, Instagram, or Twitter, for example. But even if we conclude that the social network is a filing system in the Directive's meaning, the definition still does not address the essence of such a system: it is not de-centralized (a feature which is covered in the definition). It is a distributed system, in the sense that each node can act on its own, independently of the other nodes. The operator of the social network does have technical control but, at least in current social networks, it is not applied as to the content of the personal data one user reveals to another. On the contrary: the operators of the

automated personal data systems present a serious potential for harmful consequences, including infringement of basic liberties.").

[229] *See* Weinberger, *supra* note 111.

[230] *See* SOLOVE, *supra* note 200, at 2.

[231] *See* Tene & Polonetsky, *supra* note 194.

[232] JONATHAN ZITTRAIN, THE FUTURE OF THE INTERNET AND HOW TO STOP IT 205 (2008).

systems enable—and encourage—many features, which assist users to publish data about other users, tag their photos, and much more.

A third example of the Directive's database-based shortcoming is that there are emerging technologies which do not use a database at all, but nevertheless process our personal data. These systems act upon the data immediately, rather than store it in a database, such as biometric identification methods. There are many possible ways to structure the biometric identification system.[233] One option is to collect the data from identified people (via fingerprints, facial features or iris scan) and store them in a database. Later on, when the police or the border control wish to identify a person, they can compare his or her features ""please place your index fingers here") to those stored in the database. Another option is to collect the data but store it only in a chip, which is then included within the identification document, such as a passport. The police or any other authorized agency can compare the data stored in the chip to the real features of the person. The result is the possibility to authenticate the identity, i.e., to conclude whether the person is who she says she is. Such use processes personal data without a database (Note that this is data that the subject has less control over. It is difficult to change one's finger prints or facial features.). Privacy is implicated in such systems even though there is no database. A legal regime which assumes a database is insufficient.

*

We have examined the building blocks of the Data Protection Directive: the definitions of personal data, processing, the players at stake, and the definition of a filing system. I conclude that the current legal structure uses technology-neutral language and manages to cover most technologies in current use. Nevertheless, the Directive assumes a digital environment of a certain kind, a linear processing of data destined to be included in a database. We already see a few technologies that challenge this structure, and we are likely to see more such technologies in the coming years.

CONCLUSION

Drafting legislation in a technologically-neutral manner is a much sought after goal. However, regulating technology and trying to be agnostic to the law's subject matter at the same time seems to

[233] *See* Vassiliki Andronikou, Angelos Yannopoulos & Theodora Varvarigou, *Biometric Profiling: Opportunities and Risks*, *in* PROFILING THE EUROPEAN CITIZEN, *supra* note 195, at 131.

be an impossible mission. This article suggested an interpretive method of reverse engineering the law, meant to expose the law's hidden assumptions about the regulated technology, i.e., the law's technological mindset. To the extent that we manage to uncover the hidden assumptions of the law in such a manner, we pierce the façade of the law's technology neutrality. Neutrality has its benefits, and I proposed that we evaluate it according to three justifications: flexibility, innovation and harmonization. We also saw that the legislative choice is richer than the binary neutral/specific option. But neutrality is not always attainable.

In order to shed light on the hidden technological mindset and to illustrate the benefits of reverse engineering the law, the article examined the case of informational privacy law. This emerging legal field is at an important crossroad. The United States is reexamining its approach, and the European Union is deliberating substantive amendments to its Data Protection regime. One important aspect in shaping the law and updating it is the law's stance regarding technology.

Applying the interpretive mode of reverse engineering the law to the EU Directive, the main finding was that although the Directive purports to be technology-neutral and to a great extent it is so, it does have some hidden technological assumptions. The data protection regime, as well as the proposed amendments, is within a digital technological paradigm rather than an analogue one. This is progress, of course, but we can begin noting the limits of the digital paradigm.

As long as we are within the digital paradigm, the Directive will manage to cope with new technologies that are within this technological paradigm. However, once the current technological paradigm will be replaced with a newer one (as it is bound to be), and once we will experience a transformative technology,[234] the entire data protection regime will require rethinking, not just occasional amendments. At that point, we will realize that the law was not technology-neutral. We should keep in mind the technological paradigm within which the Directive and much of data protection law elsewhere operate. Once we face new technologies that break the boundaries of the digital paradigm, the Directive is unlikely to be sustained in its current form.

---

[234] *See, e.g.*, Brenner, *supra* note 57, at 43. The standard definition of transformative technologies refers to them as general-purpose technologies, which are "characterized by the potential for persuasive use in a wide range of sectors and by their technological dynamism."). *Id. See also* Timothy F. Bresnahan & Manuel Trajtenberg, *General Purpose Technologies* "*Engines of Growth?*", 65 J. ECONOMETRICS 83, 84 (1995).

In the meantime, the level of abstraction, function-based definitions, structure of informational privacy law and especially its leading engine, the European Directive, enables the law to remain valid. Concretization of the various principles is needed, and such detailing often requires responses to particular technologies. The Article 29 Working Party provides general professional guidance on new technologies: take, for example, its view on social networks or geo-location technologies. Specific decisions are made by data protection authorities and on occasion by courts *ex post*. This structure enables the law to remain general and principled, and to proceed with specific, case-based application.

The discussion also suggests a few future research directions: looking to the past, legal history of data protection law is likely to yield interesting patterns. Looking to the future, the proposed amendments in the United States and in the EU require attention. Especially intriguing is the principle of Privacy by Design. It has become popular and is now formally on the discussion table – but it requires much unpacking. Finally, new technologies should be studied. We should explore their embedded values so as to figure out their privacy tendencies and see if these fit the law's technological mindset. Once the match no longer applies, we need to fix either the technology or the law.