Winter 2007

Twilight of the Idols? EU Internet Privacy and the Post Enlightenment Paradigm

Mark F. Kightlinger
University of Kentucky College of Law, mfkigh2@email.uky.edu

Twilight of the Idols? EU Internet Privacy and the Post Enlightenment Paradigm

ARTICLES

TWILIGHT OF THE IDOLS? EU INTERNET PRIVACY AND THE POST ENLIGHTENMENT PARADIGM

Mark F. Kightlinger[*]

This Article provides a timely examination of the European Union's approach to information privacy on the internet, an approach that some legal scholars have held up as a model for law reform in the United States. Building on the author's recent piece discussing the U.S. approach to internet privacy, this Article applies to the EU's internet privacy regime a theoretical framework constructed from the writings of philosopher and social theorist Alasdair MacIntyre on the failures of Enlightenment and post-Enlightenment thought. The EU internet privacy regime is shown to reflect and reinforce three key elements of the "post-Enlightenment paradigm," i.e., the sovereign individual, the market, and the administrative bureaucracy. The EU regime, like the U.S. internet privacy regime, stems from and helps to preserve a world in which the individual constructs a personal identity by trading personal information as a commodity to corporate bureaucracies in a regulated market under the supervision of impersonal government bureaucracies. In what MacIntyre labels "the culture of bureaucratic individualism," each new assertion of the individual's supposed fundamental right to privacy paradoxically enhances bureaucratic power. Because in these fundamental respects the EU internet privacy regime resembles the U.S. regime, the Article contends that debate over which regime is superior is little more than a family quarrel, a quarrel that cannot be resolved under the post-Enlightenment paradigm. This Article identifies and discusses important new questions about the extent to which our post-Enlightenment situation constrains our capacity to imagine and act upon innovative approaches to personal privacy.

[*] Assistant Professor, University of Kentucky College of Law; Partner, Covington & Burling 1999-2004; J.D., Yale Law School, 1988; Ph.D., Yale University, 1991; B.A./M.A., Cambridge University, 1983/1995; B.A., Williams College, 1981. I would like to acknowledge the invaluable research assistance of Caroline Henderson.

I. INTRODUCTION 2
II. THE POST-ENLIGHTENMENT PARADIGM AND THE U.S. INTERNET PRIVACY REGIME 2
III. THE EU INTERNET PRIVACY REGIME 2
A. Overview of Data Protection Directive 2
B. Consent Often Is Unnecessary 2
1. Consent to Process Ordinary PII 2
2. Consent to Use "Sensitive" PII 2
3. Consent to Transfer PII Outside the EU 2
C. Consent Is Never Enough 2
1. Data Processing Licensed by the State 2
2. Data Quality Requirements 2
3. Information Requirements 2
4. Rights of Access, Correction, and Objection 2
5. Security Measures 2
D. Consent under the ECDP Directive 2
E. EU Internet Privacy—The Bottom Line 2
IV. EU PRIVACY LAW AND THE POST-ENLIGHTENMENT PARADIGM 2
A. Individuals & Consent 2
B. Ambivalence Towards PII: Markets & Fundamental Rights 2
C. Impersonality, Bureaucracy, and the Administration of Privacy 2
1. Privacy and the Bureaucratic Business Organization 2
2. Privacy and Public Administration 2
V. THE PRIVACY DEBATE AS FAMILY FEUD 2
VI. CONCLUSION 2

I. INTRODUCTION

In recent years, there has been a constant flow of news stories reporting the lack of privacy safeguards for personally identifiable information (PII)—i.e., information about identified or identifiable persons —collected through electronic networks such as the Internet and held in electronic databases.[1] As a consequence, the U.S. legal regime for protecting such PII has encountered criticism from privacy advocates and scholars.[2] In a leading casebook on e-commerce law, for example, Professors Mann and Winn describe the "apparent consensus" within the Organization for Economic Cooperation and Development (OECD) on "the importance of information privacy and . . . of taking all appropriate steps to increase individual privacy rights."[3] In contrast to this consensus, they underscore the "sharp divisions within the U.S. debate on information privacy and the tortured progress of information-privacy law

[1] On March 14, 2007, a search via http://news.google.com detected 158 news stories containing the terms "Internet," "privacy," and "violation" posted between February 12 and March 14, 2007. There is no reason to believe that this represents an unusual number of stories for a one-month period.

[2] For examples of such criticism, see Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193 (1998), and Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609 (1999).

[3] RONALD J. MANN & JANE K. WINN, ELECTRONIC COMMERCE 209 (2d ed. 2005).

reform in the United States."[4] Critics often point to the legal regime of the European Union (EU), which adopted comprehensive privacy legislation in 1995 and special privacy legislation for electronic communications in 2002,[5] as a model for law reform in the United States.[6] Not surprisingly, this line of argument emphasizes the differences between the U.S. and EU regimes while providing legal scholars with a flattering opportunity to kibitz participants in the legislative process. This Article adopts a different strategy, highlighting features that the U.S. and EU privacy regimes have in common and explaining the significance of these common features.

In a recent article,[7] I showed that the U.S. internet privacy regime reflects and reinforces what I have termed the post-Enlightenment paradigm for explaining and justifying human action and social institutions. The post-Enlightenment paradigm emerged after the disintegration of a widely shared ancient and medieval approach to questions about human nature and ethical conduct and the subsequent failure of Enlightenment thinkers and their successors to provide a persuasive alternative.[8] Drawing extensively on the work of Alasdair MacIntyre, I argued that the post-Enlightenment paradigm relies on three elements—the individual, the market, and the bureaucracy—and their interconnections to explain and justify our actions and social institutions, and I demonstrated that these elements provide the structure for the U.S. internet privacy regime. The primary objective of this Article is to establish that the EU regime also is constructed around these three elements. Because both regimes reflect and reinforce the post-Enlightenment paradigm, a second objective of this Article is to show that disagreement over the relative merits of the two regimes is in fact a family feud.[9] My third objective is to show that such disagreement is itself a reflection of the post-Enlightenment paradigm, which channels political debate into a running battle over whether and to what extent we should expand bureaucratic power in order to limit the freedom of individuals in the market. The U.S. internet privacy regime emphasizes individual freedom, the EU regime bureaucratic power, and together they mark out and define the political alternatives that we normally have available to us.

Typically, a work of legal scholarship would proceed from this comparative discussion to a "normative" argument that one of the two internet privacy regimes, U.S. or EU, or a hybrid of them is preferable. For reasons that will become clear,[10] the post-Enlightenment paradigm commits us to the position that any such normative argument favoring one particular regime will stem from arbitrary, even if strongly held, premises and therefore draw arbitrary, even if logically sound, conclusions. One could of course purport to reject the post-Enlightenment paradigm and build a new or different intellectual foundation for a regime to protect privacy online. But doing so would require one to accomplish the philosophical task at which all

---

[4] *Id.*

[5] For a detailed discussion of the EU regime, *see infra* Part III.

[6] *See infra* notes 302–306 and accompanying text.

[7] Mark F. Kightlinger, *The Gathering Twilight? Information Privacy on the Internet in the Post-Enlightenment Era*, 24 J. MARSHALL J. COMPUTER & INFO. L. 353 (2007).

[8] *See infra* Part II (summarizing earlier discussion of the post-Enlightenment paradigm).

[9] *See infra* Part V.

[10] *See infra* pp. 58–59.

Enlightenment and pre-Enlightenment thinkers have by hypothesis failed, i.e., constructing a philosophical position that provides adequate reasons for embracing a list of moral and ethical precepts by which each of us should live. That Promethean undertaking is beyond the scope of this Article.[11] Instead, this Article pursues the more modest objective of showing that some important features of our intimate lives, including the personal relationships that to a considerable extent define who we are, elude the grasp of the post-Enlightenment paradigm's conceptual apparatus. Thus, the Article provides grounds for concluding that we may need an alternative paradigm that does not rely on the individual, the market, and the bureaucracy to explain and justify our actions and our institutions, but the Article does not attempt to supply such a paradigm.

This Article is the second step in a larger project to develop a heuristic and critical framework for investigating and appraising the historical and philosophical assumptions underlying certain modern legal and administrative arrangements. My decision to build the framework on the work of Alasdair MacIntyre is based on a conviction that legal scholarship has never adequately addressed or incorporated his insights into the origins of modernity. One might, therefore, say that this Article is my second experiment in "applied MacIntyre," testing the hypothesis that we can learn a great deal about the EU internet privacy regime and about ourselves as potential subjects of it by focusing on various issues and concerns that I have drawn from MacIntyre's work in articulating the post-Enlightenment paradigm. I reserve for a later date any effort to criticize MacIntyre's position. Instead, this Article focuses, as did the earlier article about the U.S. regime, on building a *prima facie* case for paying greater attention to MacIntyre's views in future discussions of our legal and administrative situation.

The argument of this Article proceeds in four stages. Part II summarizes the results of my previous study outlining the post-Enlightenment paradigm and showing the extent to which the U.S. internet privacy regime reflects and reinforces it. Part III describes the far more complex EU internet privacy regime, focusing on the central position of administrative bureaucracy and the relatively limited role of individual consent. Part IV shows that the EU regime reflects and reinforces the post-Enlightenment paradigm. Through careful examination of a field that is excluded from the EU regime's scope, i.e., collection and use of PII in our "purely personal" lives, Part IV also investigates certain important limitations of the post-Enlightenment paradigm. Part V argues that the alleged choice between the U.S. and EU regimes is itself a reflection of the paradigm, and that under the paradigm any choice between the two regimes ultimately will be arbitrary.

---

[11] *See infra* pp. 60–62 (briefly describing the type of argument necessary to transcend the post-Enlightenment paradigm).

II. THE POST-ENLIGHTENMENT PARADIGM AND THE U.S. INTERNET PRIVACY REGIME

Drawing on the work of Alasdair MacIntyre,[12] I argued in a recent article[13] that the internet privacy regime developed by the Federal Trade Commission (FTC) in the United States reflects and reinforces the post-Enlightenment paradigm[14] for explaining and justifying human action. The post-Enlightenment paradigm emerged after a much older tradition of reflection on ethical conduct collapsed and such Enlightenment and post-Enlightenment philosophers as Denis Diderot, David Hume, Immanuel Kant, Adam Smith, Jeremy Bentham, and John Stuart Mill failed to develop a persuasive replacement.[15] The older tradition, founded by Plato and Aristotle and sustained by later thinkers such as Thomas Aquinas, explained and justified human action using a three-part teleological framework: an account of human beings as they happen to be here and now, an account of the end or *telos* of human life, i.e., the human good, and an account of the precepts mandating certain virtues and forbidding certain vices that enable human beings to make the transition from the former to the latter.[16] Within this older tradition, ethics as a field of inquiry taught us how to understand and reflect upon our lives as they are here and now and at the same time provided us with guidance on how to achieve our potential, our good, as human beings.[17] The older tradition viewed human beings as essentially social: we embody in our lives a series of interconnected roles and relationships, each with associated precepts about virtues and vices, in and through which we develop our characters and work to realize the human *telos*.[18] At the broadest level of organization, we can become citizens of a "community united in a shared vision of the good for man (as prior to and independent of any summing of individual interests)."[19]

The older Aristotelian tradition began to crumble in the face of criticisms of teleological explanation by Reformation theologians and the emerging community of natural scientists and natural philosophers.[20] According to MacIntyre, a key effect of such criticisms was to undermine the then-existing accounts of the human *telos*,

---

[12] *See, e.g.*, ALASDAIR MACINTYRE, AFTER VIRTUE (2d ed. 1984) [hereinafter MACINTYRE, AFTER VIRTUE]; ALASDAIR MACINTYRE, WHOSE JUSTICE? WHICH RATIONALITY? (1988); ALASDAIR MACINTYRE, THREE RIVAL VERSIONS OF MORAL ENQUIRY 226 (1990) [hereinafter MACINTYRE, THREE RIVAL VERSIONS]; ALASDAIR MACINTYRE, FIRST PRINCIPLES, FINAL ENDS AND CONTEMPORARY PHILOSOPHICAL ISSUES (1990); and ALASDAIR MACINTYRE, DEPENDENT RATIONAL ANIMALS (1999).

[13] *See* Kightlinger, *supra* note 7.

[14] The term "paradigm" is borrowed from the work of Thomas Kuhn. *See* THOMAS S. KUHN, THE STRUCTURE OF SCIENTIFIC REVOLUTIONS 43–51, 174–191 (2d ed. 1970). *See also* THOMAS S. KUHN, *Second Thoughts on Paradigms*, *in* THE ESSENTIAL TENSION 293, 297, 318–319 (1977). For a discussion of Kuhn's use of the term, *see* Kightlinger, *supra* note 7, at 355 n. 9.

[15] *See* Kightlinger, *supra* note 7, at 357.

[16] *See id.*

[17] *See id.*

[18] *See id.* Thus, I might be a son today and a father tomorrow, a student today and a teacher tomorrow. To achieve my good, I would move from being a good son to a good father, a good student to a good teacher. In practicing the characteristic virtues of son, father, teacher and student, I would be contributing to the good of the relationships and organizations in which I participate.

[19] MACINTYRE, AFTER VIRTUE, *supra* note 12, at 236.

[20] Kightlinger, *supra* note 7, at 358 n. 17.

thereby replacing the three-part teleological framework with a two-part framework consisting of an account of human beings as they are here and now and one or more lists of precepts about ethical conduct that human beings should follow.[21] Enlightenment thinkers and their successors tried to provide a persuasive explanation of how these two elements of the framework might be rationally connected. Their efforts inevitably failed, however, because precepts that were intended to change and improve human beings as they are here and now simply could not be derived from any plausible account of how human beings actually are here and now.[22] As Enlightenment thinkers and their immediate successors struggled with this problem, it seemed increasingly obvious that there was an unbridgeable gap between the "is" of how human beings are here and now and the "ought" of how human beings should behave. Eventually, the "is" comes to be seen as the realm of "fact," which is objectively available for study by the natural and social sciences, while the "ought" comes to be seen as the realm of "value," which is private, subjective and not open to rational dispute.[23] The supposed gap between "is" and "ought," "fact" and "value," lies at the heart of the post-Enlightenment paradigm.

The post-Enlightenment paradigm for explaining and justifying human action has three essential elements. First, it seeks to account for human beings by treating them as individuals,[24] unlike the older teleological tradition, which treated people as instances or embodiments of human nature and as occupants of interlocking social roles and relationships.[25] As individuals, human beings may consent to play particular roles and adopt particular values, but there is no higher standard such as the human *telos*, no shared vision of the good, against which these individual decisions might be measured. Each individual has his or her own private values, and society is the arena in which each individual pursues those values in cooperation or conflict with other individuals. The model for such a society is the market, which is the second essential element of the post-Enlightenment paradigm.[26] We learn to see our social interactions as a form of market behavior in which we each pursue our individual values and the market distributes whatever we want to each of us for a price.

The challenge for any framework that attempts to explain and justify human action in terms of individuals pursuing individual values is that it appears destined to result in a world of conflict and, perhaps, chaos. The classical description of this can be found in Thomas Hobbes's charter myth of the "warre . . . of every man, against every man."[27] Adding the institution of the market to explain and justify individual interactions may account for the absence of conflict when individuals can reach mutually acceptable bargains, but there remains a need for a third element, an institution that can channel and coordinate individual activity, and thereby reduce, if not eliminate, the possibility of conflict and chaos when bargaining does not produce

---

[21] *See id.* at 357.
[22] *See id.* at 357–58.
[23] *See id.* at 359–60.
[24] *See id.* at 360–61.
[25] *See id.* at 357–58.
[26] *See id.* at 360–61.
[27] THOMAS HOBBES, LEVIATHAN 64 (Dent 1965) (1651).

acceptable results. Under the post-Enlightenment paradigm, bureaucracy provides the neutral, impersonal institution that channels and coordinates individual behavior toward pre-defined ends.[28] The bureaucracy performs this function in both business organizations and public administration. But bureaucracies do not claim to apply an objectively true standard such as a shared vision of the good to their ends because in our post-Enlightenment era such a standard is not available. In that sense, the ends that bureaucracies pursue are as arbitrary, subjective, and non-rational as the individual values those bureaucracies seek to channel and coordinate.[29] Bureaucracies do, however, maintain order, by force if necessary, and that is their function under the paradigm.

MacIntyre characterizes the symbiotic relationship between individual and bureaucracy as the "culture of bureaucratic individualism."[30] He observes that in this culture—our culture—political debate typically focuses on the merits of extending bureaucratic control.[31] Some advocate less bureaucracy and greater individual freedom to pursue individual values. Others explicitly or implicitly advocate more bureaucracy in order to "limit the free and arbitrary choices of individuals."[32] Political disputants are thus two sides of the same post-Enlightenment coin operating within the same framework but deploying conflicting and typically irreconcilable values to reach conflicting and contradictory conclusions.

The U.S. internet privacy regime reflects and reinforces the three essential elements of the post-Enlightenment paradigm. As fashioned by the FTC, the U.S. regime treats the privacy of PII as a question of individual interest and concern.[33] Each adult individual is presumed to have the ability, and thus is given the authority, to determine whether the level of protection for PII offered by a particular website is sufficient. The U.S. regime requires the website to provide whatever protection might have been promised, but the regime does not purport to question whether the level itself was sufficient.[34] That decision is left to each individual.

The U.S. regime incorporates the second element of the post-Enlightenment paradigm, i.e., the market, by presuming the existence of a market for PII, then identifying and purporting to correct a market malfunction that may arise from overly aggressive competitive behavior.[35] Specifically, the FTC treats the statements that website operators make about how they protect the privacy of PII as a form of

---

[28] *See* Kightlinger, *supra* note 7, at 361–62. For a discussion of how the term "bureaucracy" is being used here, see *id.* at 402–03, *and infra* notes 244–49 and accompanying text.

[29] *See* Kightlinger, *supra* note 7, at 361–62.

[30] MACINTYRE, AFTER VIRTUE, *supra* note 12, at 71.

[31] *See* Kightlinger, *supra* note 7, at 362.

[32] MACINTYRE, AFTER VIRTUE, *supra* note 12, at 35. Of course, those who advocate limiting freedom may speak of the need to ensure that individual behavior obeys certain rules, but in practice, this typically means that the bureaucracy's authority as the enforcer of the rules will expand. As the authors of one casebook have written, administrative agencies "are necessary if government is to do anything." JOHN M. ROGERS ET AL., ADMINISTRATIVE LAW 1 (2003).

[33] *See* Kightlinger, *supra* note 7, at 394–99.

[34] For a description of how the U.S. regime operates, *see id.* at 367–76.

[35] *See id.* at 383–89.

advertising that is potentially false and/or misleading to internet users.[36] The FTC then penalizes website operators whose collection and/or use of PII fails to abide by the operators' public statements about privacy protection.[37] The presumption is that each individual will be able to agree to a market price for his or her PII provided he or she receives accurate information about how the PII will be collected and used. PII is understood to be a commodity that can be valued in relation to other commodities.[38] Thus, paradoxically, in response to concerns that PII does not receive sufficient privacy protection on the internet, the FTC developed a legal regime designed to guarantee that PII can circulate in a properly functioning market for the right price, i.e., the price at which an adult individual who has received accurate information might agree to sell. In this respect, the U.S. regime betrays a fundamental ambivalence about the privacy of PII, extolling the value of PII but ensuring that it is for sale.[39]

The central role of the bureaucracy—the third essential element of the post-Enlightenment paradigm—in the U.S. internet privacy regime is implicit in what already has been said about the first two elements. The assumption that the value to be assigned to the privacy of PII is what each individual says it is leads to a multiplicity of possible values. Corporate bureaucracies succeed in reducing this multiplicity to a small range of possible values by offering to trade for PII at a price that serves the corporation's interests.[40] Company officials who establish the price structure at, for example, Amazon.com exercise significant influence over the value that the market will assign to the privacy of PII, thereby channeling and coordinating individual values into a relatively small range of market prices. But the threat that individuals and/or business organizations run by bureaucracies may engage in overly aggressive market behavior creates a need for another bureaucracy the task of which is to administer the rules of trade governing the market, including the key rule that website operators must abide by their public statements concerning PII. Accordingly, FTC officials play a necessary channeling and coordinating role as impersonal experts who apply a supposedly neutral system of rules to maintain order in the market.[41] Thus, it appears that under the post-Enlightenment paradigm, an individual's personal information can receive the privacy protection that the individual's private values may demand only if impersonal public officials supervise the markets where individuals disseminate their PII for a price. In this respect, therefore, the U.S. internet privacy regime reflects and reinforces the culture of bureaucratic individualism that, according to MacIntyre, pervades our modern, post-Enlightenment situation.

The next three parts of this Article show that the EU internet privacy regime represents a further step along the continuum of political debate under the post-Enlightenment paradigm. Part III outlines the EU regime, focusing on the limited

---

[36] *See id.* at 367–68.

[37] *See id.*

[38] *See id.* at 384–85.

[39] For a discussion of the ambivalence of the U.S. regime toward PII and privacy, see *id.* at 399–402.

[40] *See id.* at 403–05.

[41] *See id.* at 405–07.

role of individual consent and the central role of public officials under EU privacy law. Part IV shows the extent to which the post-Enlightenment paradigm provides the conceptual framework for the EU regime. Part V demonstrates that debate over the relative merits of the EU and U.S. internet privacy regimes will inevitably be a family feud because the two regimes and the contrasts between them are rooted in the culture of bureaucratic individualism and the post-Enlightenment paradigm.

III. THE EU INTERNET PRIVACY REGIME

The EU regime for protecting the privacy of PII on the internet consists primarily of two laws, the Data Protection Directive ("DP Directive" or "Directive")[42] and the Electronic Communications Data Protection ("ECDP") Directive.[43] The DP Directive, which was adopted in 1995, establishes uniform information privacy rules across all sectors of the economy and, with some notable exceptions, all fields of government activity—a so-called "horizontal" regime.[44] All EU Member States[45] are required to have laws on their books implementing the Directive.[46]

The ink was barely dry on the DP Directive when European officials concluded that special rules were required to address certain data-protection issues that, in their view, had begun to arise in connection with new telephone technologies such as integrated services digital networks and digital mobile telephony. Consequently, in 1997 the European Community[47] (EC) adopted the Telecommunications Data Protection ("TDP") Directive, which established privacy rules for the

---

[42] Council Directive 95/46, On the Protection of Individuals with Regard to the Processing of Personal Data, 1995 O.J. (L 281) 31 (EC) [hereinafter DP Directive]. For a general discussion of the DP Directive and its background, see Paul M. Schwartz, *European Data Protection Law and Restrictions on International Data Flows*, 80 IOWA L. REV. 471 (1995), and Spiros Simitis, *From the Market to the Polis: The EU Directive on the Protection of Personal Data*, 80 IOWA L. REV. 445 (1995).

[43] Council Directive 2002/58, Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector, 2002 O.J. (L 201) 37 (EC) [hereinafter ECDP Directive].

[44] *See* DP Directive, *supra* note 42, art. 3.2 (noting the fields of government activity to which the Directive "shall not apply" and thereby implying that it will apply to all other fields).

[45] When the DP Directive was adopted, there were fifteen EU Member States: Austria, Belgium, Denmark, Finland, France, Germany, Greece, Ireland, Italy, Luxembourg, the Netherlands, Portugal, Spain, Sweden, and the United Kingdom. Ten countries joined the EU on May 1, 2004: Cyprus, the Czech Republic, Estonia, Hungary, Latvia, Lithuania, Malta, Poland, the Slovak Republic, and Slovenia. Two more countries – Bulgaria and Romania – joined on January 1, 2007. For a short official history of the EU's growth, see Europa, The EU at a Glance – The History of the European Union, http://europa.eu/abc/history/index_en.htm (last visited Sept. 25, 2007).

[46] DP Directive, *supra* note 42, art. 32.1. The European Commission maintains a website that reports on the implementation status of the Directive in each Member State. *See* Data Protection, Status of Implementation of Directive 95/46, *available at* http://ec.europa.eu/justice_home/fsj/privacy/law/implementation_en.htm (last visited Sept. 25, 2007).

[47] The European Community ("EC") is a subordinate component of the European Union ("EU"). The EU encompasses what are commonly referred to as three "pillars": (1) the European Communities (*i.e.*, the EC, the Coal and Steel Community, and Euratom), (2) the Common Foreign and Security Policy, and (3) Cooperation in Justice and Home Affairs. For a brief discussion of the three pillars, *see* Koen Lenaerts, *Federalism: Essential Concepts in Evolution – The Case of the European Union*, 21 FORDHAM INT'L L.J. 746, 751 (1998). The EC has developed the most elaborate body of law, usually termed "EC law" or "Community law."

telecommunications sector.[48] Ironically, the TDP Directive reached the end of the legislative process at roughly the time that the internet began to emerge as a medium of communication and commerce for consumers within the EU. Not surprisingly, the TDP Directive's language, which was directed at telephony, fit internet technology poorly.[49] Thus, when European officials embarked on an effort in 2000 to update laws related to electronic communications, they proposed to revise the TDP Directive to address internet issues. Following this revision process, the EC replaced the TDP Directive with the ECDP Directive in 2002.

Since the ECDP Directive was written to cover the internet, it would seem natural to focus on that law in this Article. That approach would be misguided, however, because most issues that may arise between internet users and website operators are likely to arise not under the narrowly targeted ECDP Directive, but under the horizontal DP Directive. Thus, this Article focuses on the latter. The Article briefly discusses the ECDP Directive in order to show how it supplements the DP Directive.[50]

A. Overview of Data Protection Directive

The DP Directive imposes a range of obligations on "data controllers," i.e., the people within an organization who determine the purposes and means for processing personal data.[51] This Article focuses on website operators who collect and use personal data and who therefore are data controllers under the Directive.[52] The phrase "personal data" covers all "information relating to an identified or identifiable natural person," or "data subject."[53] Member State officials charged with enforcing the Directive tend to interpret the concept of "personal data" expansively. In the internet context, for example, a bare IP address[54] in the hands of a website operator

---

[48] Council Directive 97/66, Concerning the Processing of Personal Data and the Protection of Privacy in the Telecommunications Sector, 1998 O.J. (L 24) 1 (EC) [hereinafter TDP Directive].

[49] For example, under the TDP Directive, network operators generally were required to erase or make anonymous "traffic" data generated in the course of connecting "calls." TDP Directive, *supra* note 48, art. 6.1. In the Internet context, it makes little sense to refer to the communication between an individual and a website as a "call" and thus it was unclear whether and to what extent the TDP Directive's restrictions on traffic data applied to websites. For a more detailed discussion of this issue, see Mark F. Kightlinger et al., *International Privacy*, *in* E-COMMERCE LAW & BUSINESS 10–08 to 10–00 (Mark E. Plotkin et al. eds., 2003).

[50] *See infra* Part D.

[51] DP Directive, *supra* note 42, art. 2(d). The Directive's requirements apply to all persons or organizations that may collect and use an individual's PII, with one exception. The Directive does not apply to processing of personal data "by a natural person in the course of a purely personal or household activity." *Id.* art. 3.2. The Directive also does not cover data collection and use related to "public security, defence, State security . . . and the activities of the State in areas of criminal law." *Id.* art. 3.2. *See infra*, note 88, for a short discussion of the Directive's national defense and security loopholes.

[52] Although the Article focuses on the obligations that the Directive imposes on website operators, it should not be misunderstood to imply that these obligations relate exclusively or specifically to website operators. The obligations apply generally to all individuals and entities that are, or wish to become, data controllers.

[53] *Id.* art. 2(a). In order to avoid over-reliance on the Directive's technical jargon, this Article uses the term "PII" as a synonym for "personal data."

[54] "[A]n IP address identifies a computer connected to the Internet with a unique . . . number made up of 12 digits divided into four groups of numbers separated by decimals – *e.g.*, 121.122.123.124." MANN & WINN, *supra* note 3, at 756.

may be considered personal data on the theory that "someone, somewhere can connect the IP address to an individual internet user."[55] The Directive also defines the term "processing" broadly to cover essentially any operation that a data controller might perform on PII from collection through deletion.[56]

Under the Directive, each EU Member State must establish a data protection supervisory authority (DPSA) "responsible for monitoring the application within its territory of the provisions adopted by the Member States pursuant to this Directive."[57] The Directive says little about the composition of the DPSAs except that they must be "public authorities," i.e., administrative agencies.[58] The Directive appears to presume that the DPSA will consist of "members and staff,"[59] suggesting a bureaucratic structure comprising a manager or management group such as a board or commission overseeing the work of subordinate officials. The DPSAs "shall act with complete independence in exercising the functions entrusted to them."[60] They should not, in other words, be subject to external political or administrative control. Member State law must give the DPSA power to investigate, including "access to data forming the subject-matter of processing operations."[61] Thus, PII is not protected from, or private with respect to, the DPSA. Member States must ensure, however, that the members and staff of the DPSA are "subject to a duty of professional secrecy with regard to confidential information to which they have access."[62] In addition, the DPSA can opine on data protection policy, bring administrative proceedings against data controllers, and take data controllers to court for alleged violations of applicable laws.[63] The DPSA must have the power to "order[] the blocking, erasure or destruction of data, [and] . . . impos[e] a temporary or definitive ban on processing."[64] Administrative decisions by supervisory authorities may be appealed to national courts.[65]

The DP Directive establishes a Working Party on the Protection of Individuals with regard to the Processing of Personal Data (DPSA Working Party) comprising a representative of each DPSA, a representative from any EC-level data protection authority, and a representative of the European Commission.[66] The Directive gives the DPSA Working Party a range of responsibilities. For purposes of this Article, the most important is to "examine any question covering the application of the national measures adopted under this Directive in order to contribute to the uniform

---

[55] Kightlinger, *supra* note 49, at 10–25 (footnote omitted).

[56] DP Directive, *supra* note 42, art. 2(b). This Article refers to "collection and use" of PII rather than "processing of personal data," but these phrases are intended to be synonymous.

[57] *Id.* art. 28.1.

[58] *Id.*

[59] *Id.* art. 28.7.

[60] *Id.* art. 28.1.

[61] *Id.* art. 28.3.

[62] *Id.* art. 28.7. It is not clear whether the phrase "confidential information" is intended to cover all of the PII to which the DPSA might have access or only a portion of the PII that is deemed "confidential."

[63] *Id.* art. 28.3.

[64] *Id.*

[65] *Id.*

[66] *Id.* arts. 29.1, 29.2. For information about the composition of the DPSA Working Party, see Justice and Home Affairs, Data Protection – Working Party – Members, http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/members_en.htm.

application of such measures."[67] In carrying out this responsibility, the DPSA Working Party has adopted more than one hundred papers interpreting the Directive and discussing its application to various privacy issues.[68] Although the legal status of these papers is not clear, they do provide valuable guidance to anyone interested in finding out how the DPSAs interpret the Directive and intend to enforce its terms.[69]

As discussed in the following parts, under the DP Directive, a person's informed consent is often unnecessary and never sufficient to legitimate collection and use of PII. Informed consent is often unnecessary because in a variety of circumstances, a website operator is not required to obtain a person's consent before collecting and using the person's PII. Instead, the website operator must meet the requirements and expectations of the relevant DPSA. Consent is never enough because a website operator must fulfill a number of obligations before, during, and after collecting and using PII that are independent of the consent of any person whose PII the controller may collect. Those obligations facilitate oversight by the DPSA that enforces them. Indeed, it is only a slight overstatement to say that the primary purpose of the Directive is to subject collection and use of PII to comprehensive administrative oversight while providing space for informed consent where it appears that individuals can be trusted with decisions concerning the handling of their own PII. This arrangement may be contrasted with that in the United States, where the primary purpose of the bureaucracy in the field of privacy protection is to facilitate and establish the conditions for individual consent. What the two systems have in common is that they are both forms of bureaucratic individualism, as one would expect under the post-Enlightenment paradigm.

B. Consent Often Is Unnecessary

Under the DP Directive, a data controller is allowed to collect and use PII only if the controller can identify a legitimate basis for doing so.[70] Consent is one such basis. A website operator who wishes to collect and use an individual's PII may rely on an individual's consent in three situations. A website operator may seek—but is not required to seek—consent when collecting or using what might be called

---

[67] DP Directive, *supra* note 42, art. 30.1(a).

[68] For links to all of the papers that the DPSA Working Party has adopted since 1997, see Justice and Home Affairs, Data Protection – Documents Adopted by the Data Protection Working Party, http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2006_en.htm (last visited Sept 25, 2007).

[69] For example, in a recent opinion, after a lengthy discussion of a particular company's alleged violations of Belgian and/or European law, the DPSA Working Party issued a blunt threat: "[i]n case of non-compliance, data controllers can expect to be subject to sanctions imposed by the competent authorities under the Directive and national law, in order to enforce compliance." DPSA Working Party, *Opinion 10/2006 on the Processing of Personal Data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT)* 27 (Nov. 22, 2006), *available at* http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2006/wp128_en.pdf.

[70] The prohibition on collection and use without a legitimate basis is explicit in regard to "special" categories of PII, DP Directive, *supra* note 42, art. 8.1 and recital 33, but implicit in regard to other types of PII, *id.* art. 7 ("Member States shall provide that personal data may be processed only if . . ."). *Id.* recital 30.

"ordinary" PII.[71] The Directive strongly encourages but does not require a website operator to seek consent when collecting and using what the Directive labels "special" categories of PII.[72] Finally, a website operator may seek—but is not required to seek—consent when transferring PII to a data controller located in a non-EU country that fails to provide "adequate" protection for PII.[73] In each of these situations, it is clear that a website operator also may collect and use a person's PII without consent, if the operator relies on one of the other legitimate bases approved by the Directive.

1. Consent to Process Ordinary PII

Article 7 of the DP Directive enumerates the conditions under which a person or entity, including a website operator, may make "legitimate"[74] use of an individual's ordinary[75] PII. Not surprisingly, a website operator may use PII if "the data subject has unambiguously given his consent."[76] The Directive defines "the data subject's consent" as "any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed."[77] It is generally believed that opt-out consent[78] is sufficiently "unambiguous" and thus that consent may be implied from a person's decision to submit PII in response to an appropriate request from a data controller.[79] As discussed below, implied consent will not suffice for collection and use of "sensitive" PII.[80]

The DP Directive allows a website operator to collect and use ordinary PII without consent if one of several conditions is satisfied. A website operator may collect and use an individual's PII without consent to (1) perform a contract with the individual,[81] (2) comply with a "legal obligation,"[82] or (3) protect the individual's "vital interests."[83] The Directive also permits a website operator to use an individual's PII without consent if the "processing is necessary for the purposes of the legitimate interests pursued by the [website operator] . . . , except where such interests are overridden by the interests or fundamental rights and freedoms of the

---

[71] *See infra* Part 1.

[72] *See infra* Part 2.

[73] *See infra* Part 3.

[74] Article 7 falls within Part II, which is entitled "Criteria for Making Data Processing Legitimate." DP Directive, *supra* note 42, section II. Article 7 requires that "Member States shall provide that personal data may be processed *only* if" one of six enumerated conditions is satisfied. *Id.* art. 7 (emphasis added).

[75] The DP Directive does not identify particular categories of PII as "ordinary." As discussed in Part 2, *infra*, however, the Directive does characterize certain categories of PII as "sensitive" or "special." As used in this Article, the term "ordinary" refers to PII that does not qualify for the higher level of protection granted to "sensitive" PII. Most types of PII would be considered "ordinary" in this sense.

[76] DP Directive, *supra* note 42, art. 7(a).

[77] *Id.* art. 2(h).

[78] "Opt-out" consent arises when a person must take an affirmative step to forbid collection and use of PII. *See* MANN & WINN, *supra* note 3, at 758.

[79] *See* Kightlinger, *supra* note 49, at 10–33.

[80] *See infra* Part 2.

[81] DP Directive, *supra* note 42, art. 7(b).

[82] *Id.* art. 7(c).

[83] *Id.* art. 7(d).

data subject . . . ."[84] This provision has been called the "business purposes" rule because it permits a website operator to collect and use someone's PII for the website operator's own purposes without consent.[85] The website operator's purposes must be "legitimate," which means in practice that the website operator must be able to persuade the relevant DPSA that the purposes are legitimate, if the website operator's activities are challenged.[86] Moreover, the website operator's purposes must yield if they conflict with the individual's "fundamental rights and freedoms," an undefined phrase to which DPSAs will give meaning in particular cases, subject of course to judicial review.[87] Given the central role of the DPSA in determining the parameters of the "business purposes" rule, it is fair to say that the rule effectively replaces an individual's consent to a particular use of PII with the DPSA's view of whether such use is appropriate. The rule transforms a transaction between an individual and a website operator into a transaction between a website operator and the DPSA.[88]

One might respond that the individual's consent is relevant to one, if not two, of the supposedly non-consensual bases for collecting and using ordinary PII. Consent typically would be present if a website operator collects and uses PII to fulfill a contract with the individual from whom PII was collected. Consent arguably also is present if the website operator uses an individual's PII for "business purposes," because the individual would not have provided the PII if he or she did not consent—at least tacitly—to its collection and use for the purposes indicated by the business. According to this argument, consent is irrelevant only if the website operator collects a person's PII to meet a "legal obligation" or protect the person's "vital interests." Although a website operator might be able to abuse these bases for

---

[84] *Id.* art. 7(f).

[85] *See* Kightlinger, *supra* note 49, at 10–31.

[86] DPSAs have the power to hear complaints, DP Directive, *supra* note 42, art. 28.4, and institute proceedings against alleged violators, *id.* art. 28.3. Thus, to avoid further enforcement proceedings, a website operator typically will have to persuade the DPSA that a particular use of PII is legitimate. Regardless of any action by the DPSA, however, individuals may seek a "judicial remedy for any breach of the rights" granted under the Directive, *id.* art. 22, including compensation for damages, *id.* art. 23.1.

[87] For discussions of judicial review of agency action in the EU and Member States, see Jürgen Schwarze, *Judicial Review of European Administrative Procedure*, 68 LAW & CONTEMP. PROBS. 85 (2004); Claudia Tobler, Note, *The Standard of Judicial Review of Administrative Agencies in the U.S. and EU: Accountability and Reasonable Agency Action*, 22 B.C. INT'L & COMP. L. REV. 213 (1999). For a broader discussion of judicial review of Member State actions under EU law, see HENRY G. SCHERMERS & DENIS F. WAELBROECK, JUDICIAL PROTECTION IN THE EUROPEAN UNION 644–52 (6th ed. 2001).

[88] The Directive establishes a sixth condition under which it is legitimate to collect PII that is not pertinent here. PII may be processed if "processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed." DP Directive, *supra* note 42, art. 7(e). This provision is one of several significant loopholes permitting government officials to collect and use PII more or less as they see fit. *See, e.g., id.* art. 3.2 (exempting from the Directive's coverage all data "processing operations concerning public security, defence, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law . . ."). Member State authorities are notably less forgiving when, for reasons of national security, U.S. government officials seek to collect and use PII related to Europeans. *See* Belgian Commission for the Protection of Private Life, *Summary of the Opinion on the Transfer of Personal Data by SCRL SWIFT Following the UST (OFAC) Subpoenas*, Sept. 27, 2006, *available at* http://www.privacycommission.be/communiqués/summary_opinion_Swift_%2028_09_2006.pdf.

collecting and using PII, they hardly represent gaping loopholes in a regime that otherwise seems to emphasize consent.

There is merit to this response. Consent does matter under the DP Directive. An individual may limit use of PII by refusing consent. At the same time, this response must confront one seemingly insurmountable objection based on the express language of the Directive. Article 7 specifically identifies "unambiguous consent" as one legitimate basis among several for collecting and using ordinary PII. Although it is possible to find evidence of consent or consent-like behavior—perhaps this might be termed "ambiguous consent" —with respect to at least two of the other bases, Article 7 expressly treats these other bases as distinct, and therefore different, from unambiguous consent. Thus, it is misleading to claim that these non-consensual bases nevertheless require or presuppose informed consent. Of course, one can always argue that the decision to submit PII reflects a person's consent to submit PII. But this is a tautology, not a legal argument, and as such, it implies nothing about the rules that govern use of the person's PII. Indeed, as discussed below,[89] it is clear that under many, if not most, circumstances a person's consent, however unambiguous, does not and cannot define or limit the person's rights or the rights and obligations of the website operator, because those rights and obligations are not established by consensual agreement. Rather, the rights and obligations are established almost exclusively by the law itself as interpreted by the relevant DPSA.

2. Consent to Use "Sensitive" PII

Under Article 8 of the Directive, with narrow exceptions discussed below, "Member States shall prohibit the processing of personal 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."[90] The Directive refers to these as "special categories of data"[91] or "sensitive"[92] PII. The Directive does not explain why these particular categories warrant heightened protection,[93] and it makes no provision for people who believe that some of these categories do not need such protection. The Directive also makes no allowance for people who believe that an unlisted category of PII is "special" and deserves heightened protection. One such omitted category is personal financial information. In the United States, under many circumstances, an individual's financial information receives special legal protection.[94] Under the Directive, financial

[89] *See infra* Part C.

[90] DP Directive, *supra* note 42, art. 8.1.

[91] *Id.* section III.

[92] *Id.* recital 34.

[93] The Directive simply asserts, in a recital, that personal "data which are capable by their nature of infringing fundamental freedoms or privacy should not be processed" except under narrowly defined conditions. *Id.* recital 33.

[94] John C. Dugan et al., *Privacy and E-Commerce in the United States*, in E-COMMERCE LAW & BUSINESS 9–96 to 9–915 (Mark E. Plotkin et al. eds., 2003). *See also* U.S. GOVERNMENT ACCOUNTABILITY OFFICE, PERSONAL INFORMATION: KEY FEDERAL PRIVACY LAWS DO NOT REQUIRE INFORMATION RESELLERS TO SAFEGUARD ALL SENSITIVE DATA (June 2006), *available at* http://www.gao.gov/new.items/d06674.pdf (recommending that Congress require information resellers to provide greater protection for sensitive personal information, particularly financial information).

information receives no special protection. Similarly, PII related to children receives special protection in the United States under the Children's Online Privacy Protection Act (COPPA)[95] but is treated as ordinary PII under the Directive. Of course, the general level of protection under the Directive is relatively high, so failure to designate a particular category as "special" does not mean that the category receives no legal protection. But if the Directive's list of "special" categories seems strangely arbitrary, this is because the list imposes a legislative decision about the categories of PII that a person *should* value more highly instead of empowering people to make such decisions for themselves.

A website operator or other data controller may collect and use "special" or "sensitive" PII under any of five narrowly defined conditions. One condition—discussed in greater detail below[96]—is with the individual's explicit consent. A website operator may collect and use such PII without consent (1) to abide by obligations under employment laws;[97] (2) in the "vital interests" of a person who "is physically or legally incapable of giving his consent";[98] (3) under certain conditions if the website operator is a non-profit social organization such as a church or a union;[99] or (4) if the PII was "manifestly made public" or is necessary to establish or defend "legal claims."[100] The Directive permits Member States to establish, either by law or through their DPSAs, other conditions under which a website operator can collect and use "special" categories of PII without consent "for reasons of substantial public interest."[101] "Substantial public interest" comprises "areas such as public health and social protection—especially in order to ensure the quality and cost-effectiveness of the procedures used for settling claims for benefits and services in the health insurance system—scientific research and government statistics."[102] For purposes of this Article, there are three important points to make about these non-consensual bases for collecting sensitive PII. First, they are narrowly drawn, and this indicates that EU legislators knew how to push controllers to obtain consent when they wished to do so. The Directive's emphasis on consent for collecting sensitive PII contrasts markedly with the Directive's approach to ordinary PII, where legislators approved broadly worded alternatives to consent. Second, the list of non-consensual bases for collecting sensitive PII appears to reflect a belief that the state's administrative apparatus is the primary legitimate consumer of such PII. Hence, such PII may be collected as required by employment law or as needed by public

---

[95] 15 U.S.C. §§ 6501–6506 (2000). For a general discussion of COPPA, see Kightlinger, *supra* note 7 at 372–76; *see also* Dugan, *supra* note 94, at 9–94 to 9–96.

[96] *See infra* notes 103 to 110 and accompanying text.

[97] DP Directive, *supra* note 42, at art. 8.2(b).

[98] *Id.* art. 8.2(c). It is worth noting that the "vital interests" exception to the prohibition on use of sensitive PII is much narrower than the "vital interests" basis for using ordinary PII. *See id.* art. 7(d) (omitting the requirement that the person be "physically or legally incapable of giving his consent"). This suggests, among other things, that a website operator may be allowed to collect and use PII without a person's consent to protect the person's allegedly vital interests even if the website operator could have obtained consent. It will fall to the DPSA to determine whether the person's interests were "vital" and whether those interests were protected.

[99] *Id.* art. 8.2(d).

[100] *Id.* art. 8.2(e).

[101] *Id.* art. 8.4.

[102] *Id.* recital 34.

institutions pursuing allegedly public interests. Third, the DPSA, not the individual, has final authority to determine whether to establish new non-consensual bases for collecting and using sensitive PII. Thus, whether a particular category of PII is sensitive ultimately depends not on how the individual values his or her own PII but on how DPSA officials value such PII.

Although the DP Directive allows collection and use of sensitive PII with the individual's consent, the Directive betrays a notable lack of confidence in the individual's capacity to exercise that consent wisely. The Directive allows use of sensitive PII if the individual "has given his explicit consent to the processing of those data, except where the laws of the Member State provide that the prohibition . . . may not be lifted by the data subject's giving his consent."[103] This provision is illuminating in two respects. First, it requires "explicit" consent, unlike the parallel consent provision for ordinary PII.[104] In the online context, this means that "opt in"[105] consent is required to collect and use sensitive PII.[106] Thus, before collecting such PII, a website operator must provide a consent form containing the terms on which PII will be used, and persuade the individual to signify acceptance of those terms by, for example, clicking a button that says "I ACCEPT." This suggests that EU legislators were willing to give the individual consensual authority over his or her sensitive PII, but only if the individual is confronted with an "in your face" consent form designed to discourage carelessness and inattention. Apparently, individuals were not trusted to handle their own sensitive PII with sufficient care and attention. Moreover, as the Directive strengthens the hand of the internet user, it also enhances the role of the DPSA, which retains the ultimate authority, backed by national and EU courts, to determine whether the words contained in the website operator's consent form are satisfactory, i.e., sufficiently "explicit," in the Directive's terms. The mere fact that a person clicked "I ACCEPT" before providing sensitive PII will not settle the question.

Second, the consent provision for sensitive PII is illuminating because it expressly permits EU Member States to limit or eliminate consent as a basis for collecting and using sensitive PII. In a Member State that followed this course, a person might not be permitted to authorize use of his or her own PII if it falls into one of the categories that the Directive deems "sensitive." This would mean, for example, that I might not be permitted to authorize Amazon's United Kingdom website (Amazon.UK)[107] to record my interest in gay-themed literature and films, because this could be deemed "processing of data concerning . . . sex life."[108] It

---

[103] *Id.* art. 8.2(a).

[104] *See supra* note 76 and accompanying text. It follows that the Directive permits "implicit" or tacit consent for use of ordinary PII.

[105] "Opt-in" consent arises when an organization has to obtain an individual's express permission before collecting and using his or her PII. *See* MANN & WINN, *supra* note 3, at 758.

[106] Kightlinger, *supra* note 49, at 10–03 to 10–04.

[107] Amazon's web address in the United Kingdom actually is Amazon.co.uk, but I shorten it to Amazon.UK in the Article for the sake of simplicity.

[108] DP Directive, *supra* note 42, art. 8.1. To readers outside the EU, this assertion may seem somewhat farfetched. In fact, it is well within the realm of Member State practice. In one well-known case, the Swedish data protection authority found that an airline computerized reservation service had violated the law by recording the fact that a passenger preferred kosher food. According to the authority,

would not be legally relevant that I may not regard this information as "sensitive" or "special," or that I may want Amazon to record my interest in such books and films in order to provide me with updates when new materials of interest are published.

Most Member States have chosen to recognize consent as a basis for collecting and using sensitive PII.[109] Nevertheless, it is revealing that EU lawmakers agreed that a Member State reasonably could refuse to allow a person to consent to the use of certain categories of his or her own PII. In effect, the Directive allows a Member State to grant itself sole control over decisions about collection and use of precisely those types of PII that the Directive declares to be "capable by their nature of infringing fundamental freedoms or privacy."[110] Thus, when the risk to personal privacy is supposedly greatest, the Directive consistently shows a lack of confidence in the individual's capacity to look after his or her own interests. It empowers the DPSA to protect the person's privacy not only from aggressive website operators but from the person himself or herself.

3. Consent to Transfer PII Outside the EU

One important purpose of the DP Directive was to ensure that PII could not be transferred out of the EU without strong assurances that it would continue to receive legal protection.[111] Accordingly, the Directive imposes an export-control regime on international data transfers. The interplay between consent and DPSA oversight under this regime is sufficiently complex and interesting to warrant a separate article that also would examine the impact of efforts to extend the geographical reach of the Directive extraterritorially to certain controllers located outside the EU.[112] For

---

this preference tended to reveal that the passenger's religious beliefs, and therefore constituted sensitive PII under the Directive. *See* DPSA Working Party, *Recommendation 1/98 on Airline Computerised Reservation Systems (CRS)* 4 (Apr. 28, 1998), *available at* http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/1998/wp10_en.pdf (explicit consent required to collect sensitive data concerning religious dietary preferences).

[109] *See* Douwe Korff, *EC Study on Implementation of Data Protection Directive Comparative Study of National Laws* 86–68 (Sept. 2002), *available at* http://ec.europa.eu/justice_home/fsj/privacy/docs/lawreport/consultation/univessex-comparativestudy_en.pdf; *See also* European Commission, Analysis and Impact Study on the Implementation of Directive EC 95/46 in Member States 12, *available at* http://ec.europa.eu/justice_home/fsj/privacy/docs/lawreport/consultation/technical-annex_en.pdf.

[110] *See supra* note 93.

[111] *See* DP Directive, *supra* note 42, recital 57 ("transfer of personal data to a third country which does not ensure an adequate level of protection must be prohibited"); *see also* DPSA Working Party, *Working Document: Transfers of Personal Data to Third Countries: Applying Articles 25 and 26 of the EU Data Protection Directive* 8 (July 24, 1998), *available at* http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/1998/wp12_en.pdf (a "missing element" of the Council of Europe's 1981 Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data "is the absence of restrictions on transfers to countries not party to it").

[112] The Directive asserts extraterritorial legal authority over controllers who are "not established on Community territory and, for purposes of processing personal data make use of equipment, automated or otherwise, situated on the territory of the said Member State . . ." *Id.* art. 4.1(c). According to the DPSAs, under this provision, EU/Member State law will apply to a website operator based outside the EU who collects PII directly from individuals residing in the EU after placing a small text file called a "cookie" on the individual's computer. DPSA Working Party, *Working Document on Determining the International Application of EU Data Protection Law to Personal Data Processing on the Internet by Non-EU Based*

purposes of this Article, however, it is important to note only the salient features of the regime. The Directive tightly restricts most transfers of PII from the EU to a "third country," which for practical purposes means any country that is outside the European Economic Area.[113] Such transfers are permitted without restriction only if the third country "ensures an adequate level of protection."[114] The Directive does not define the term "adequate" and provides limited guidance concerning how adequacy is to be assessed.[115] The Directive authorizes the European Commission, working in cooperation with a committee of Member State officials, to make adequacy determinations.[116] Once the Commission determines that a third country provides adequate protection, a website operator is permitted to transfer a person's PII to a data controller in that country without the person's consent or any other special protections.[117]

If a website operator wishes to transfer PII to a data controller in a third country such as the United States that has not been deemed to provide adequate protection by EU standards,[118] the operator is faced with an array of legal options similar to those discussed above[119] for collecting and using ordinary PII. The operator may

---

Web Sites 10–01 (May 30, 2002), *available at* http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2002/wp56_en.pdf.

[113] *See* Kightlinger, *supra* note 49, at 10–01. The European Economic Area contains the 27 Member States of the EU plus Iceland, Liechtenstein, and Norway. The Directive frequently uses the phrase "third country" or "third countries" but does not provide a definition. *See, e.g.*, DP Directive, *supra* note 42, recitals 20, 37, 56, and arts. 19.1(e), 25, 26.

[114] *Id.* art. 25.1.

[115] *Id.* art. 25.2.

[116] *Id.* arts. 25.6, 31.2. To date, the Commission has found that three countries – Argentina, Canada, and Switzerland – and two dependencies of the British Crown – Guernsey and the Isle of Man – provide adequate protection for PII. *See* Commission Decisions on The Adequacy of The Protection of Personal Data in Third Countries, http://ec.europa.eu/justice_home/fsj/privacy/thridcountries/index_en.htm. The EU-U.S. Safe Harbor Agreement establishes a set of privacy principles that a U.S.-based company can adopt voluntarily in order to be deemed to provide adequate protection for PII exported from the EU. For the U.S. Commerce Department's explanation of the Safe Harbor Agreement, see U.S Commerce Department, Welcome to Safe Harbor, http://www.export.gov/safeharbor (last visited October 4, 2007).

[117] DP Directive, *supra* note 42, art. 25.

[118] To date, the European Commission has never made a formal finding that the level of protection in a third country is inadequate. Thus, despite suggestions to the contrary in the secondary literature, *see e.g.*, MANN & WINN, *supra* note 3, at 215, there is no finding that the level of protection in the United States is not adequate by EU standards. Clearly, however, it was a premise of the negotiations that led to the adoption of the EU-U.S. Safe Harbor Agreement, *see supra* note 116 and accompanying text, that the general level of protection for PII in the United States is not adequate. Reflecting this view, the DPSA Working Party has stated that "the patchwork of narrowly focused sectoral laws and self-regulatory rules presently existent in the United States cannot be relied upon to provide adequate protection in all cases for personal data transferred from the European Union." DPSA Working Party, *Opinion 2/99 on the Adequacy of the "International Safe Harbor Principles" Issued by the US Department of Commerce on 19th April 1999*, at 2 (May 3, 1999) *available at* http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/1999/wp19en.pdf. Concurring in this view, Professors Schwartz and Reidenberg stated that "[t]he treatment of personal information in the U.S. private sector does not always fulfill the standards of protection found in the European principles." Paul M. Schwartz & Joel R. Reidenberg, DATA PRIVACY LAW 396 (1996). *See* Patrick J. Murray, Comment, *The Adequacy Standard Under Directive 95/46/EC: Does U.S. Data Protection Meet This Standard*, 21 FORDHAM INT'L L.J. 932, 1013–3017 (1998) (arguing U.S. privacy protection in private sector is generally not adequate by EU standards).

[119] *See supra* Part I.

undertake such a transfer if the individual has "given his consent unambiguously."[120] The operator may transfer PII without consent (1) to perform a contract between the website operator and the individual, or to implement "precontractual measures"; (2) to conclude or perform a contract "concluded in the interest of the data subject between the controller and a third party"; (3) when "necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims"; (4) to protect the individual's "vital interests"; or (5) when the transfer originates from a public register of PII.[121] Although this is not the place for a detailed discussion of these provisions, it should be clear that a savvy website operator—or a website operator with a savvy attorney—often will be able to rely on them to transfer PII without an individual's consent to third countries that lack adequate protection.

The Directive also allows a website operator to transfer PII without consent to a third country that lacks adequate protection "where the controller adduces adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights[;] such safeguards may in particular result from appropriate contractual clauses."[122] Under this "adequate safeguards" provision, the website operator "adduces" the safeguards not to the person whose PII will be transferred but to DPSAs and/or European Commission officials who determine whether the safeguards are legally adequate.[123] Some DPSAs require that contractual safeguards for international transfers be pre-approved on a case-by-case basis, while others will allow a website operator to export PII under self-imposed safeguards until challenged to defend them.[124] The Directive also authorizes the European Commission to approve "standard contractual clauses"[125] that will be deemed to provide adequate safeguards for transfers to data controllers in countries lacking adequate protection. To date, the Commission has approved two such standard clauses.[126] In practice, website operators and other data controllers treat the Commission's standard clauses as the baseline for adequacy.[127] One point should be clear from this description of the

---

[120] DP Directive, *supra* note 42, art. 26.1(a). "Unambiguous" consent for an international transfer may be tacit or opt-out consent in most instances. *See supra* note 104 and the accompanying text.

[121] DP Directive, *supra* note 42, arts. 26.1(b)–(f).

[122] *Id.* art. 26.2.

[123] Article 26.2 states that safeguards must be "adduced" but does not say to whom. The website operator clearly does not have to adduce safeguards to the individual whose PII the operator plans to export. The "adequate safeguards" rule is an alternative to consent, so the individual typically is out of the loop. The remainder of Article 26 leaves little doubt that DPSAs and the European Commission are in charge. Under Article 26.3, "[t]he Member State shall inform the Commission and the other Member States of the authorizations it grants pursuant to paragraph 2." *Id.* art. 26.3.

[124] *See* Kightlinger, *supra* note 49, at 10–05.

[125] DP Directive, *supra* note 42, art. 26.4. The procedure for adopting standard contractual clauses, *id.* art. 31(2), involves consultation with a committee of "representatives of the Member States . . . chaired by the representative of the Commission." *Id.* art. 31.1.

[126] Commission Decision of 15 June 2001 on Standard Contractual Clauses for the Transfer of Personal Data to Third Countries, Under Directive 95/46/EC, 2001 O.J. (L 181) 19; Commission Decision of 27 December 2001 on Standard Contractual Clauses for the Transfer of Personal Data to Processors Established in Third Countries, Under Directive 95/46/EC, 2002 O.J. (L 6) 52. The Directive defines a "processor" as "a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller." DP Directive, *supra* note 42, art. 2(e).

[127] *See* Kightlinger, *supra* note 49, at 10–06.

"adequate safeguards" regime: the consent of the individual plays no role. A website operator who "adduces" such safeguards may transfer an individual's PII to a third country without seeking the individual's consent. Here again, administrative control by the DPSA substitutes for individual consent and defines the space within which consent may operate.

C. Consent Is Never Enough

Under the DP Directive, the informed consent of a person is never sufficient to ensure that a website operator may collect and use the person's PII lawfully. This is because the Directive imposes a panoply of obligations on website operators that have little or nothing to do with a person's consent. As briefly discussed in the following Subparts, these include requirements to (1) obtain a license from or register with a DPSA to process PII; (2) satisfy various "data quality" requirements; (3) provide a variety of information to the individual whose PII is to be collected; (4) grant the individual access to his or her PII, and the opportunity to correct mistaken information; and (5) adopt security measures to protect PII.[128] Although consent plays a limited role in the Directive's treatment of some of these requirements, the requirements do not flow from the individual's consent. Failure to comply with any of these requirements is a separate violation, and the DPSA Working Party has taken the position that an individual cannot release a website operator from these requirements by consent in, for example, the context of a contractual agreement.[129]

1. Data Processing Licensed by the State

The Directive requires a prospective data controller such as a website operator to notify the relevant DPSA prior to any "wholly or partly automatic" collection or use of PII.[130] It is only a slight exaggeration to call this prior notification requirement a licensing regime. The Directive requires each Member State to identify those types of "processing operations likely to present specific risks to the rights and freedoms of data subjects" and to "check that these processing operations are examined prior to the start thereof."[131] Such checking may be carried out either by the DPSA or the controller's in-house "data protection official,"[132] if any. It

---

[128] These issues are discussed *infra* in Parts 1 through 5.

[129] *See* DPSA Working Party, *Opinion 1/98: Platform for Privacy Preferences (P3P) and the Open Profiling Standard (OPS)* 1 (June 16, 1998), *available at* http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/1998/wp11_en.pdf.

[130] DP Directive, *supra* note 42, art. 18.1. At a minimum, the notification must include (1) the website operator's name and address; (2) the purpose(s) for which the operator will be processing PII; (3) the categories of people whose data the operator will process; (4) the categories of PII that the operator will process; (5) a list of recipients or categories of recipients to whom PII may be disclosed; (6) any proposed transfers to countries outside the EU; and (7) a description of the steps that the operator will take to comply with the Directive's data security requirements. *Id.* art. 19.1(a)–(f).

[131] *Id.* art. 20.1.

[132] The Member States may provide for simplified notification or exemption from notification for (1) data processing activities that the Member State deems to be low-risk and/or (2) data controllers that appoint an independent "data protection official" to oversee the controller's data processing activities. *Id.* art. 18.2. If a data controller appoints an in-house data protection official, the official is required to

clearly is accurate to say that the Directive establishes a licensing regime for processing operations subject to prior "checking," because collection and use may proceed only after the DPSA approves, explicitly or implicitly.[133] With respect to collection or use of PII not designated for prior checking, it would be more accurate to say that the Directive establishes a registration regime.[134] Thus, a registered website operator does not have to await the approval of the DPSA simply to collect and use PII, but failure to register renders such collection and use illegal.

The interplay between informed consent and registration/licensing under the DP Directive can be described in one word: nonexistent. Under the Directive, the requirement to register or obtain a license to collect and use PII is independent of any consent that a website operator may obtain to collect and use a particular person's PII. Rather, the registration/licensing requirements empower the DPSA and bring all collection and use of PII under administrative scrutiny. As the Directive states, the notification requirements "are designed to ensure disclosure of the purposes and main features of any processing operation for the purpose of verification that the operation is in accordance with the national measures taken under this Directive."[135] The use of the term "verification"[136] suggests that the DPSA should actively review registrations for compliance with national law and not simply await complaints from people injured by non-compliance.

2. Data Quality Requirements

The DP Directive requires data controllers[137] such as website operators to comply with various "data quality principles."[138] A website operator is required to

---

maintain a register of the controller's processing activities and ensure that the data controller abides by applicable law. In effect, the official stands in for the DPSA in connection with notification requirements.

[133] According to a recital, "Member States must provide that the supervisory authority, or the data protection official in cooperation with the authority, check such processing prior to it being carried out; [and] following this prior check, the supervisory authority may, according to its national law, give an opinion or an authorization regarding the processing . . .." *Id.* recital 54. The Directive does offer an alternative to such case-by-case prior authorization. A Member State may specify by law or regulation the types of data processing that place individual rights and freedoms at risk, and identify the conditions under which those types of processing may occur. The DPSA apparently will not have to pre-approve individual instances of such processing that meet the relevant conditions. *Id.*

[134] The United Kingdom's law implementing the Directive uses the term "registration" to characterize the prior notification system. *See* Data Protection Act, 1998, ch. 29, § 18, *available at* http://www.opsi.gov.uk/acts/acts1998/19980029.htm [hereinafter UK Data Protection Act].

[135] DP Directive, *supra* note 42, recital 48.

[136] The French version of the Directive uses the term "*contrôle*" where the English version uses the term "verification." Thus, the French version indicates that the DPSA should use registration information to exercise "control" over data processing activity that does not comply with French law. Directive 95/46/CE du Parlement Européen et du Conseil du 24 Octobre 1995 Relative à la Protection des Personnes Physiques à l'Égard du Traitement des Données à Caractêre Personnel et à la Libre Circulation de ces Donneés, recital 48, *available at* http://ec.europa.eu/justice_home/fsj/privacy/docs/95-56-ce/dir1995-56_part2_fr.pdf (second part). Under the case law of the European courts, "a particular provision [of EC legislation] should not be considered in isolation but in cases of doubt should be interpreted and applied in the light of the other official languages." Case T-80/97, Starway v. Council, 2000 E.C.R. II-3099 (EU).

[137] DP Directive, *supra* note 42, art. 6.2 (imposing on data controllers the requirement to comply with data quality principles).

[138] *Id.* section I (entitled "Principles Relating to Data Quality").

ensure that PII is (1) "processed fairly and lawfully"; (2) "collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes"; (3) "adequate, relevant and not excessive in relation to [those] purposes"; (4) "accurate and, where necessary, kept up to date"; and (5) "kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed."[139] These principles are stated in very general terms and the Directive provides almost no guidance concerning their interpretation. The principles clearly have little to do with consent, and a great deal to do with the authority of the DPSA.

The requirement that PII be collected and used "fairly" provides a good illustration.[140] A recital provides the Directive's only gloss on this requirement: "if the processing of data is to be fair, the data subject must be in a position to learn of the existence of a processing operation and, where data are collected from him, must be given accurate and full information, bearing in mind the circumstances of the collection."[141] It seems unlikely, however, that EU legislators would have chosen a general term such as "fair" if what they meant was "not secret" or "not properly informed." The DPSA Working Party has stated that "[f]or personal data to be processed fairly they must be processed in a way that does not bring about unfairness to the data subject. This is potentially a very wide-ranging requirement."[142] Not surprisingly, the DPSA Working Party has opined that in some circumstances collection and use of PII "may be unfair even if the [individual] has consented."[143] Indeed, there is evidence to suggest that the DPSAs believe the fairness principle gives them broad authority to mandate specific practices as "fair" and prohibit other practices as "unfair."[144] Citing fairness and other data quality principles, the DPSAs

---

[139] *Id.* art. 6.1(a)–(e).

[140] *Id.* art. 6.1(a).

[141] *Id.* recital 38.

[142] DPSA Working Party, *Opinion 8/2001 on the Processing of Personal Data in the Employment Context* 18 (Sept. 13, 2001), *available at* http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2001/wp48en.pdf.

[143] *Id.*

[144] For examples of the Working Party's use of the fairness principle to impose detailed requirements on collection and use of PII, see DPSA Working Party, *Working Document Privacy on the Internet – An Integrated EU Approach to On-line Data Protection* 37 (Nov. 21, 2000), *available at* http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2000/wp37en.pdf (unfair to use an email address "collected in a public space on the Internet" for direct marketing purposes); DPSA Working Party, *Recommendation 2/2001 on Certain Minimum Requirements for Collecting Personal Data On-line in the European Union* 6–6 (May 17, 2001), *available at* http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2001/wp43en.pdf (unfair to collect PII online before providing specified list of information); DPSA Working Party, *Working Document on Determining the International Application of EU Data Protection Law to Personal Data Processing on the Internet by Non-EU Based Web Sites* 13 (May 30, 2002), *available at* http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2002/wp56_en.pdf (fairness requires "the individual should have the possibility to accept or refuse the placing of a cookie and . . . to determine what data he wishes to be processed by the cookie"); DPSA Working Party, *Sixth Annual Report on the Situation Regarding the Protection of Individuals with Regard to the Processing of Personal Data and Privacy in the European Union and in Third Countries* 29 (Dec. 16, 2003), *available at* http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2003/2003–3th-annualreport_en.pdf (under "principles of fair and lawful use, the data subject has to be informed every time a creditor makes an entry into the reporting system"); DPSA Working Party, *Opinion 5/2004 on Unsolicited Communications for Marketing Purposes under Article 13 of Directive 2002/58/EC* 6 (Feb. 27, 2004), *available at*

have prescribed in considerable detail the terms under which a website operator may collect and use PII.[145]

3. Information Requirements

The DP Directive requires a data controller such as a website operator to supply specified information when collecting an individual's PII. The operator must disclose: (1) the operator's identity; (2) the purposes for which the PII is being collected and used; and (3) "any further information . . . in so far as such further information is necessary . . . to guarantee fair processing in respect of the data subject."[146] The Directive provides three examples of such "further information": (1) "the recipients or categories of recipients of the data;" (2) "whether replies to the questions are obligatory or voluntary, as well as the possible consequences of failure to reply;" and (3) "the existence of the right of access to and the right to rectify the data."[147]

At first blush, the Directive's information requirements cast doubt on this Article's argument that informed consent takes a back seat to bureaucratic control under the Directive. Surely the purpose of the information requirements is to ensure that an individual receives detailed notice about how his or her PII will be used prior to consenting to its collection. The information requirements thus assist a person in providing a "freely given specific and informed indication of his wishes"[148] concerning collection and use of PII. There is, of course, some truth to this claim. The information requirements do help to ensure that, insofar as a person's consent is legally relevant under the Directive, information will be available on which the person can base that consent. What is lacking in the Directive, however, is any suggestion that there is a legal relationship between the information requirements and the individual's consent, or that compliance with the information requirements will suffice to ensure that an individual's consent is informed. On the contrary, the Directive's references to consent are contained in provisions that are entirely separate from the Directive's information requirements.[149] A DPSA may treat failure to supply the requisite information as a violation regardless of whether the individual's consent was the legal basis for collecting and using the individual's PII.

---

http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2004/wp90_en.pdf (email harvesting unlawful because, inter alia, unfair).

[145] For an example of the highly detailed requirements that the DPSAs may seek to impose on a website operator such as Microsoft, see DPSA Working Party, *Working Document on On-line Authentication Services* 6–61 (Jan. 29, 2003), *available at* http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2003/wp68_en.pdf. The author should disclose here that at one time he represented Microsoft on data protection issues in the EU. He played no role in the negotiations that culminated in the arrangements outlined in the foregoing paper by the DPSA Working Party.

[146] DP Directive, *supra* note 42, art. 10(a)–(c).

[147] *Id.* art. 10(c). The Directive imposes a very similar information requirement on a website operator who collects an individual's PII from a source other than the pertinent individual (*e.g.*, a company that sells address lists or PII databases). *Id.* art. 11.1.

[148] *See supra* note 77 and accompanying text.

[149] *See* DP Directive, *supra* note 42, arts. 7(a), 8.2(a), *and* 26.1(a) (bestowing legal significance on the data subject's consent without reference to the provision of information) *and* arts. 10 and 11 (requiring provision of information without reference to the subject's consent).

Moreover, the Directive does not require a website operator to provide the information outlined in the information requirements to the individual at the time of, or in the context of, data collection. For example, at least one national law implementing the Directive appears to permit a data controller to satisfy the requirement to specify the purposes for which PII will be collected and used either by providing that information to the person from whom the PII is collected or by providing that information to the DPSA in the data controller's registration.[150] Clearly, information residing in the DPSA's registration database has a tenuous relationship at best with an individual's informed consent during a transaction with, for example, Amazon.UK. Finally, even assuming the Directive's information requirements facilitate informed consent in many situations, it is important to note that the requirements include an open-ended obligation to supply whatever details may be needed to ensure that collection and use of PII is "fair." Thus, a website operator could comply with the precise language of the information requirements, an individual could supply PII, thereby apparently consenting to its use under the terms that the operator had specified, and yet the DPSA still could take the position that the individual did not receive sufficient information to ensure that this collection and use of PII was "fair."[151] Here again, the website operator's primary concern may be to satisfy the DPSA and not to inform the individual.

4. Rights of Access, Correction, and Objection.

The DP Directive grants a person the right to access and seek correction of his or her PII. A Member State must ensure that a person has the right to confirm (1) whether or not a website operator is making use of the person's PII; (2) the purposes for which PII is being used; (3) the categories of PII in use; and (4) "the recipients or categories of recipients to whom the [PII is] disclosed."[152] In addition, Member States must give people the right to rectify or erase PII, particularly if "incomplete or inaccurate."[153] A person's consent is irrelevant to the rights of access and correction.

In addition to establishing rights of access and correction, Member States must give a person the right:

---

[150] UK Data Protection Act, *supra* note 134, sched. 1, part 2, ¶ 5.

[151] The United Kingdom's Data Protection Act, for example, states that collection and use of PII will not be considered "fair" unless the data subject is provided with the information indicated in the Directive's information requirements. *Id.* sched. 1, part II, ¶ 2(1). The Act then states that the information that must be provided includes "any further information which is necessary, having regard to the specific circumstances in which the data are or are to be processed, to enable processing in respect of the data subject to be fair." *Id.* sched. 1, part II, ¶ 2(3)(d). Thus, in order to ensure that processing is fair, the data controller must provide all information necessary to ensure that the processing is fair. The DPSA and the courts ultimately will decide how to satisfy this circular "fairness" requirement.

[152] DP Directive, *supra* note 42, art. 12(a). If the individual wishes, he or she also may obtain the PII itself "in an intelligible form" as well as details about the source of the PII. *Id.*

[153] *Id.* art. 12(b). The website operator or other data controller is also required to notify anyone to whom the individual's PII has been disclosed that rectification, erasure, or blocking has occurred, if the individual so requests and if doing so does not "prove[] impossible or involve[] a disproportionate effort." *Id.* art. 12(c).

> at least in the cases referred to in Article 7 (e) and (f), to object at any time on compelling legitimate grounds relating to his particular situation to the processing of data relating to him, save where otherwise provided by national legislation. Where there is a justified objection, the processing instigated by the controller may no longer involve those data.[154]

The "cases referred to in Article 7(e) and (f)" are among those in which a website operator may collect a person's PII without consent.[155] Thus, having granted website operators the power to collect and use a person's PII without consent, the Directive returns a measure of control by giving the person a right to find out whether a particular website operator is using his or her PII and then empowering the person to object. But it is important to note that the right to object or opt out of data collection and use is not unconditional. A person has to be able to show "compelling legitimate grounds" before his or her objection will force a website operator to stop using the person's PII. In the Directive's terminology, an objection must be "justified," and a website operator is within his or her rights to request a reason before heeding an objection. By granting the person a right to object but requiring the website operator to comply only if the objection is justified, the Directive clearly enhances the authority of the individual but also and more importantly augments the authority of the DPSA. In any particular case, the DPSA and courts, not the individual, would determine what constitutes a "justified" objection based on "compelling legitimate grounds."

5. Security Measures

In one other area, the DP Directive imposes significant requirements on website operators that are independent of the consent of an individual whose PII the operator may collect or use. Website operators and other data controllers must "implement appropriate technical and organizational measures to protect" the security of PII.[156] This is not the proper place for a detailed review of the Directive's security requirements and how they fit into the mosaic of rules that the EU has implemented in the fields of network security and cybercrime.[157] For purposes of this Article, the important point is that the Directive implicitly vests in the DPSA the responsibility for determining whether in any particular instance a website operator is providing sufficient security. Here again, the Directive assigns no legal significance to the consent of the individual whose PII is being protected. Thus, one would expect the website operator to treat website security as yet another transaction with the DPSA rather than with the individual.

---

[154] *Id.* art. 14(a). Member States also must grant the individual the right to object to use of his or her PII for "purposes of direct marketing." *Id.* art. 14(b).

[155] *See supra* notes 84 through 88 and accompanying text.

[156] DP Directive, *supra* note 42, art. 17.1. In addition to this general requirement to protect the security of PII, the Directive imposes special requirements on website operators and other data controllers who outsource processing operations. Such a website operator must enter into a contract with the third-party processor stating that the latter will act only on instructions of the former and will abide by the security requirements of the Member State in which the former is established. *Id.* art. 17.3.

[157] For a brief overview of European rules and agreements governing Internet security and cybersecurity, see D. Jean Veta et al., *Cybersecurity: Risk and Liability in the New Information Environment*, *in* E-COMMERCE LAW & BUSINESS 16–605 to 16–614 (Mark E. Plotkin et al. eds., 2003).

D. Consent under the ECDP Directive

A detailed discussion of the ECDP Directive is beyond the scope of this Article, because the ECDP Directive was intended to address a number of data protection issues that have only limited relevance to the internet.[158] Thus, for example, the ECDP Directive regulates (1) collection and use of "traffic data" generated by telephone systems and digital networks during electronic communications;[159] (2) collection and use of "location data" of the sort generated by cellular phones or other mobile electronic appliances;[160] (3) use of data in telephone and e-mail directories;[161] and (4) certain types of wire tapping or data interception.[162] The ECDP Directive introduces some kind of consent requirement or option in most of the areas that it regulates.[163] For example, in the EU, unsolicited direct marketing by e-mail is seen as a data protection issue, and the ECDP Directive tightly restricts such marketing by requiring marketers in most situations to obtain the recipients' prior opt-in consent.[164] The ECDP Directive also requires websites to give a user the opportunity to opt out of the placement of "cookies" on his or her personal computer.[165]

One might contend that the ECDP Directive's emphasis on consent casts doubt on a key argument of this Article, namely that the EU's approach to online privacy tends to substitute administration by DPSAs for individual consent. In fact, it would be more accurate to describe the ECDP Directive as the exception that proves the rule. First, the ECDP Directive is narrowly targeted at specific problems, whereas the DP Directive is horizontal and applies to all aspects of a website's collection and use of an individual's PII. Thus, the emphasis on consent in the ECDP Directive in no way undermines the claim that the DP Directive tends to empower DPSAs and limit the significance of consent. Indeed, the ECDP Directive's narrowly crafted provisions seem to signal an effort to enhance the importance of, and at the same time carefully circumscribe, individual consent. They certainly do not signal a broad shift from DPSA oversight to informed consent as the primary focus of privacy protection. Underlining this point, the ECDP Directive significantly expands the

---

[158] For more on the ECDP Directive, see Kightlinger, *supra* note 49, at 10–08 to 10–00.

[159] ECDP Directive, *supra* note 43, art. 6.

[160] *Id.* art. 9.

[161] *Id.* art. 12.

[162] *Id.* art. 5.

[163] *See, e.g. id.* arts. 6.3 (consent to use of "traffic data" to market communications services or provide enhanced services to subscribers), 9.1 (consent to use location data to provide enhanced communications services), and 12.3 (consent to allow searching of phone or email directories by identifiers other than name).

[164] *Id.* art. 13.1. The ECDP Directive carves out an important exception for e-mail that is sent to the sender's own customers, provided those customers have not objected and the e-mail concerns products or services that are similar to those that the customer already has purchased. *Id.* art. 13.2. For a detailed discussion of the EU's complex and somewhat confusing approach to marketing e-mail, see Mark E. Plotkin et al., *Consumer Protection*, *in* E-COMMERCE LAW & BUSINESS 14–43 to 14–404 (Mark E. Plotkin et al. eds., 2003).

[165] ECDP Directive, *supra* note 43, recital 25.

power of the DPSAs by authorizing them to "carry out the tasks laid down in [the DP Directive] with regard to matters covered by this Directive . . . ."[166]

Second, and related to the first, the ECDP Directive supplements the DP Directive in two ways: in some areas it fills perceived gaps in the DP Directive's regulatory structure and in others it arguably[167] alters the rules that would pertain if the DP Directive remained the applicable law. To the extent that the ECDP Directive fills gaps by, for example, introducing rules covering certain types of data that might not qualify as PII under the DP Directive,[168] the ECDP Directive's emphasis on consent tells us nothing about the significance attached to consent under the DP Directive. To the extent that the ECDP Directive alters the regime that would apply under the DP Directive by replacing or supplementing a prohibition or a mandate with a consent provision, it would appear to follow that the DP Directive itself must have attached little or no legal significance to consent in the relevant area. Otherwise, a new consent provision would not be necessary. Thus, the references to consent in the ECDP Directive support the argument that the primary effect of the DP Directive is to empower DPSAs rather than individual adult internet users.

Third, it is important to note that the EU adopted the ECDP Directive seven years after adopting the DP Directive. Based on my work as an attorney and lobbyist on privacy issues in Europe during the relevant time period, I believe that the ECDP Directive's emphasis on consent reflects the heated political debate that developed after the DP Directive was adopted. In private meetings, company officials, trade associations, and attorneys practicing in the data-protection field sought to persuade officials to make broad use of the consent language in the DP Directive and criticized official reliance on mandates and prohibitions that effectively shifted responsibility and authority from individuals to DPSAs. Perhaps recognizing the political force of claims that people should be allowed to decide for themselves whether and how their PII will be collected and used, the officials who drafted the new ECDP Directive backed away from the DPSA-centered approach of the DP Directive in several areas and interposed consent requirements.[169] This suggests a shift in mindset on the part of EU legislators—a shift that arguably was triggered in part by the hostile response in many quarters to the DP Directive. If criticism of the DP Directive was one reason for the increased emphasis on consent reflected in the more recent ECDP Directive, this too would support the argument that the DP Directive attaches limited legal significance to individual consent.

---

[166] *Id.* art. 15.3.

[167] The claim is arguable because the ECDP Directive does not purport to repeal or supersede any provisions of the DP Directive.

[168] For example, the ECDP Directive regulates use of "traffic data" that facilitate movement of communications over electronic networks but that arguably are not – or at least not always – PII covered by the DP Directive. *Id.* art. 2(b) (defining "traffic data").

[169] One also can see evidence of the increasing emphasis on consent by comparing the ECDP Directive and the law that it revised and replaced, the TDP Directive. *See supra* notes 48 and 49 and accompanying text. The latter, which was adopted in 1997, contained a variety of strict prohibitions and requirements and made minimal use of consent. Although the ECDP Directive was adopted just five years after the TDP Directive, the former made far greater use of consent requirements.

E. EU Internet Privacy—The Bottom Line

This Part of the Article shows in some detail that the EU internet privacy regime subjects website operators who collect and use PII to continuous, far-reaching administrative oversight that begins before PII is collected and ends, if at all, only after PII has been destroyed or rendered anonymous via removal of personal identifiers. The regime accomplishes this by requiring all data controllers to register with a DPSA and comply with broadly worded mandates that empower DPSAs to evaluate, influence, and in many instances control, the terms and conditions for PII collection and use. Although the DP Directive recognizes that the individual's consent can play a role in protecting the privacy of PII, the Directive permits extensive non-consensual use of PII. Consent can safely take a back seat precisely because it is the job of the DPSA, not the individual, to protect the privacy of PII from threats posed by data controllers such as website operators and, if possible, from the negative consequences of the individual's own consensual decisions.

IV. EU PRIVACY LAW AND THE POST-ENLIGHTENMENT PARADIGM

This Part examines the EU internet privacy regime in light of the account of the post-Enlightenment paradigm summarized in Part II. In particular, this Part shows that the EU regime reflects and reinforces the three key elements of the paradigm: the individualization of privacy and the attendant emphasis on consent, the fundamentally ambivalent market relationship of the individual to his or her PII, and the overarching need for expert, impersonal bureaucratic administration by corporations and public officials. Examining the EU regime in light of the paradigm also reveals some important limitations of the paradigm itself, centered around the paradigm's seeming inability to explain and justify human conduct in personal relationships of trust and intimacy.

A. Individuals & Consent

Under the post-Enlightenment paradigm, the individual becomes the primary, if not the sole, unit of social theoretical analysis[170] and thus one would expect an internet privacy regime to focus on protecting and regulating the PII of individuals. In this respect, the DP Directive clearly reflects and reinforces the post-Enlightenment paradigm. The first evidence of the Directive's focus on individuals is the title of the Directive itself: "on the protection of individuals with regard to the processing of personal data and on the free movement of such data."[171] In recitals, the Directive repeatedly announces its focus as "protection of the rights and freedoms of individuals"[172] or the "fundamental rights . . . of individuals."[173] The particular individual right that the Directive purports to protect is privacy.[174] The

---

[170] *See supra* notes 24–26 and accompanying text.

[171] DP Directive, *supra* note 42.

[172] *See, e.g., id.* recitals 7–9, 11, 68.

[173] *See, e.g., id.* recitals 3, 34, 37. *See also id.* arts. 25.6, 26.2, 26.3, 28.2 (referring in various ways to protection of the "fundamental" or "basic" rights and freedoms of individuals).

[174] *See, e.g., id.* art. 1.1 and recitals 2, 7, 9, 11 and 68; *but see id.* recital 34 (apparently distinguishing between "fundamental rights" and the "privacy of individuals").

operational provisions of the Directive do not refer to protection of the individual, but they leave no doubt that the individual is the primary, if not the sole, object of the Directive's concern. The Directive applies to the PII of the "data subject" who is "an identified or identifiable natural person," i.e., an individual.[175] PII, or "personal data" in the parlance of the Directive, is any information related to such an identified or identifiable individual.[176] The individual data subject is tantamount to the subject of a descriptive sentence, and each item of PII, each personal datum, is a predicate of that subject, which or who is always singular. Mark Kightlinger is tall, forty-seven, white, male, gay, an attorney, a professor, a writer, a brother, a son, a messy housekeeper. These predicates are personal data about the identifiable individual "Mark Kightlinger."

Also consistent with the post-Enlightenment paradigm, the DP Directive treats consent as the primary means by which the individual can exercise legal authority over collection and use of PII. The Directive effectively prohibits a website operator from collecting, using and/or exporting ordinary or sensitive PII without a recognized legal basis for doing so. One of the legal bases that the Directive recognizes in each instance is consent.[177] By implication, therefore, the Directive treats all other legal bases for collecting, using, and/or exporting PII as non-consensual.[178] Under the Directive, consent yields a "freely given specific and informed indication of [the individual's] wishes" with respect to collection and use of his or her PII.[179] Thus, consensual use of the individual's PII should reflect the individual's wishes. Part C *infra* argues that non-consensual use of PII typically will reflect the wishes of a website operator or other business organization under the supervision of a DPSA. As one would expect under the post-Enlightenment paradigm, the individual has little control over such non-consensual uses of PII. The individual has a right to be informed of such uses[180] and may express an objection to them,[181] but a website operator must heed the objection only under ill-defined circumstances that will demand DPSA oversight.

As was the case under the U.S. internet privacy regime,[182] the DP Directive's focus on individuals and consent fits awkwardly with the social reality that the Directive itself recognizes. Take one example that I briefly discussed in the U.S. context.[183] Assume that the data subject mentioned above—Mark Kightlinger (MK)—has a boyfriend named Gordon Goodlooking (GG). MK has good reason to believe that GG is gay. Under the Directive, the mere fact that MK might collect this item of sensitive PII about GG does not transform MK into a controller subject

---

[175] *See supra* note 53 and accompanying text.

[176] *See supra* notes 53–54 and accompanying text.

[177] *See supra* Part B.

[178] *See supra* notes 81–88 and accompanying text (non-consensual bases for collecting and using ordinary PII), notes 97–102 (non-consensual bases for collecting and using sensitive PII), and notes 121–127 and accompanying text (non-consensual bases for exporting PII to third countries that lack "adequate" protection).

[179] *See supra* notes 77–80 and accompanying text.

[180] *See supra* Part 3.

[181] *See supra* Part 4

[182] *See* Kightlinger, *supra* note 7, at 393–397.

[183] *Id.* at 395–396.

to the Directive's requirements. The reason is that the Directive explicitly does not cover collection or use of PII "by a natural person in the course of a purely personal . . . activity."[184] But if MK provides the item of PII "GG is gay" to a website operator, perhaps in response to a marketing survey, several provisions of the Directive would apply. For example, the website operator would be required to identify a recognized legal basis for collecting and using the PII. As discussed above, information about GG's sex life is considered "sensitive,"[185] and the rules governing sensitive PII would push the website operator to obtain GG's opt-in consent before collecting such PII from MK.[186] MK's consent to the collection of PII about GG would be legally irrelevant. Assuming the website operator had a sufficient legal basis for collecting sensitive PII about GG, the website operator would be required to inform GG, among other things, that the website operator has collected GG's PII and how the website operator plans to use the PII.[187] The fact that the website operator may have provided that same information to MK would be legally irrelevant. In other words, although the Directive expressly recognizes a space for "purely personal" activity in which one person may hold PII about another without incurring legal obligations, the Directive still assigns each item of PII to an individual when imposing rules governing consent and information. The same can be said about rules governing the individual's right to access and correct PII.[188] MK would have no right to access and/or correct GG's PII once that PII is in the possession of a controller despite the fact that the controller may have obtained the PII from MK and regardless of the nature of the relationship between MK and GG.

Thus far, perhaps, the DP Directive's emphasis on the individual's consensual authority over his or her PII may seem sensible. After all, the sentence "GG is gay" seems to recite a fact about GG, so perhaps it makes sense for the Directive to assign consensual authority over that fact to GG and not to MK, even if MK learned the fact about GG by interacting directly with GG in the purely personal space. Assume, however, that the item of PII that MK gathers in the purely personal space is not "GG is gay" but rather "GG is MK's boyfriend." This item of PII arguably is not about GG any more than it is about MK. The sentence "GG is MK's boyfriend" arguably is true if and only if the sentence "MK is GG's boyfriend" also is true.[189] Such "boyfriend" PII seems to be about both MK and GG or, perhaps more accurately, about the relationship between MK and GG. "Boyfriend" PII pertains to MK and GG as members of a couple or dyad with romantic and presumably sexual connotations rather than to MK and GG as individuals. As long as such "boyfriend" PII remains purely personal, the Directive does not assign the PII to an individual. Thus, within the purely personal space, the Directive appears to allow for the possibility of relational PII that is shared between or among people and is not subject to individual consensual control.

---

[184] *See* DP Directive, *supra* note 42, art. 3.2.
[185] *See supra* notes 90–92 and accompanying text.
[186] *See supra* Part 2.
[187] DP Directive, *supra* note 42, art. 11.1.
[188] *See supra* Part 4.
[189] *See* Kightlinger, *supra* note 7, at 396–397

Matters will be quite different, however, if MK informs a website operator such as an online travel agent that "GG is MK's boyfriend." The DP Directive then would require the website operator to confront the question whether he or she now possesses "information relating to an identified or identifiable natural person" named GG. The obvious answer would seem to be "yes." This means that under the Directive the website operator would be deemed a controller with respect to PII about an individual named GG. Accordingly, the website operator would have to identify a legal basis for collecting and using the PII, provide certain information to GG, and grant GG a right to access and correct the PII. Moreover, because the PII likely would be deemed "sensitive," it would be difficult for the website operator lawfully to collect the information "GG is MK's boyfriend" from MK without promptly obtaining GG's opt-in consent. What was PII about a couple or a relationship in the purely personal space becomes an item of "personal data" about an individual and subject to individual consent under the Directive if and when someone provides it to a third party outside the purely personal space. The nature and subject matter of the PII do not change, but as required by the post-Enlightenment paradigm, the Directive transforms shared, relational "boyfriend" PII into "personal data" about two individuals subject to each individual's consensual authority. Generalizing this point, the line that the Directive draws between the purely personal space and the space that the Directive regulates functions as a horizon or boundary that simultaneously marks the outer limits of the post-Enlightenment paradigm's reach and acknowledges a reality of shared relationships lying beyond that reach.

A possible objection to the argument thus far presented is that it depends heavily on the rather unusual nature of "boyfriend" PII and, in particular, "boyfriend" PII related to a same-sex couple. Isn't such dyadic or relational PII exceptional? A complete response to this question would take the argument too far afield, but the short answer is that such PII is not exceptional. A large majority of EU residents presumably have or at one time had mothers and fathers about whom they hold substantial amounts of PII gathered in the context of purely personal activity, including PII specifically about the parent-child relationship. A great many EU residents also hold PII about their relationships with their sisters and brothers, spouses, children, grandparents, cousins, nieces and nephews. Most—even the attorneys—also hold PII about relationships with close friends, and some hold PII about lovers. Many belong to unions, churches, political parties, and other social organizations that generate and share PII internally.[190] When I say "Pauline is my mother," "Karolena is my niece," and "Holger is my first cousin once removed," I am recording PII about relationships that partially define and constitute my status as a member of an extended family. Change the names and most, if not all, of the readers of this Article could utter similar sentences recording PII about family members, close friends, lovers, poker buddies, or fellow members of the Rotary

[190] PII related to membership in such an organization receives special treatment under the DP Directive. The organization may collect and use sensitive PII about its members for its own purposes without consent provided the PII is not transferred to third parties. DP Directive, *supra* note 42, art. 8.2(d). In this respect, therefore, such an organization receives treatment similar to that accorded the individual's "purely personal" life, which lies beyond the horizon of the Directive. *See supra* notes 184 to 187 and accompanying text.

Club. Thus, there is nothing unusual about the type of relational PII that the Directive implicitly acknowledges and exempts within the purely personal space. Indeed, for most of us, such relational PII probably tells us more about who we really are than do such institutional identifiers as an email address or a social security number. Yet under the Directive, once relational PII such as "Henry is my friend" crosses the boundary line demarcating the purely personal, it becomes "personal data" about individuals, and this is true whether it qualifies as ordinary or sensitive. The individual's primary legal authority over either type of PII is the capacity to consent (or not) to its collection and use. This is precisely what one would anticipate under a regime that reflects the post-Enlightenment paradigm and reinforces it by implementing it into law.

By drawing a line between the unregulated purely personal social reality and the regulated reality of "personal data," EU legislators seem to imply that it would be inappropriate, if not impossible, to impose on the purely personal reality the paradigmatic requirements that each item of PII be assigned to at least one individual and that the individual exercise consensual authority over collection and use of that PII. In this respect, the unregulated purely personal reality poses a challenge to the post-Enlightenment paradigm, suggesting that something about who and what we are qua participants in the purely personal reality escapes the paradigm's effort to explain and justify human action in terms of individuals consenting to trade in markets overseen by bureaucracies. Two boyfriends, for example, share PII in the intimacy of the purely personal space. They do not trade PII with one another as individuals in a market. The precepts about trust, disclosure, discretion, and mutual respect governing their use of relational PII presumably stem from their shared vision of what it means to be good boyfriends and not from the principles of market behavior, the DP Directive, or the right to privacy.[191] These brief comments are intended to draw attention to the post-Enlightenment paradigm's limitations and thus raise the possibility that an alternative paradigm might provide a more adequate explanation and justification of human action in the purely personal space. One candidate, of course, would be the older Aristotelian teleological paradigm, which assumed not that people are individuals but rather that a person's relationships to other people, e.g., family, friends, and lovers, constitute the person as who he or she is and help to define the ends that he or she should pursue in concert with others.[192] The question whether the older paradigm in fact provides a more adequate account of the purely personal space excluded by the Directive is beyond the scope of this Article as is the larger and more difficult question whether one could use the older paradigm to construct an adequate alternative account of the realm of individuals and individual consent that the Directive does regulate.

B. Ambivalence Towards PII: Markets & Fundamental Rights

In Part II, this Article noted that the U.S. internet privacy regime, which reflects the post-Enlightenment paradigm, reveals the individual's deep ambivalence toward

---

[191] *See also* Kightlinger, *supra* note 7, at 397–398 (a person who misuses his boyfriend's PII will be criticized as a bad boyfriend and not for making a bad deal in the market).

[192] *See supra* note 18 and accompanying text.

his or her PII and its privacy.[193] On the one hand, the regime signals that individuals place a high value on information privacy and experience considerable anxiety about protecting PII. On the other hand, the regime ensures that the individual can trade PII in a market to the highest bidder. The EU internet privacy regime reflects this same ambivalence by declaring that the privacy of PII is a fundamental right requiring specialized administrative oversight and at the same time promoting free movement of PII throughout the EU in a regulated market.

As previously noted, the DP Directive repeatedly declares that its purpose is to protect the "fundamental" or "basic" rights of individuals, particularly the right to privacy in regard to collection and use of PII.[194] The Directive does not, of course, purport to explain how EU legislators knew that this particular right exists or that it qualifies as fundamental and/or basic. According to the Directive, the authority for the assertion that such a right exists is pre-existing European treaty law:

> the object of the national laws on the processing of personal data is to protect fundamental rights and freedoms, notably the right to privacy, which is recognized both in Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms and in the general principles of [European] Community law.[195]

Article 8 of the European Convention states—also without explanation or argument—that "[e]veryone has the right to respect for his private and family life, his home and his correspondence."[196] The Directive does not explain how or why the fundamental right to privacy of PII derives from this "right to respect for . . . private and family life." A legal regime could pay significant respect to a person's "private and family life," covering such areas as sexual activity, child rearing, and religious practices, while providing little or no special legal protection for PII. Moreover, it is not clear how the asserted right to respect for private and family life squares with the DP Directive's exclusion of PII held in the purely personal space, which presumably comprises much of private and family life.

The DP Directive also cites as a source for the fundamental right to privacy of PII the Council of Europe's 1981 Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (DP Convention).[197] The DP Convention declares that its purpose is "to secure in the territory of each Party for every individual, whatever his nationality or residence, respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him ('data protection')."[198] Thus,

---

[193] *See supra* notes 35–39 and accompanying text.

[194] *See supra* notes 172–74 and accompanying text.

[195] DP Directive, *supra* note 42, recital 10.

[196] Council of Europe, Convention for the Protection of Human Rights and Fundamental Freedoms, art. 8(1) (Nov. 4, 1950), *available at* http://conventions.coe.int/Treaty/en/Treaties/Html/005.htm. For a discussion of the Convention, see Kightlinger, *supra* note 49, at 10–04 to 10–06.

[197] DP Directive, *supra* note 42, recital 11. *See* Council of Europe, Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (Jan. 28, 1981), *available at* http://conventions.coe.int/Treaty/en/Treaties/html/108.htm [hereinafter Data Protection Convention]. For a discussion of the Data Protection Convention, see Kightlinger, *supra* note 49, at 10–07 to 10–01.

[198] Data Protection Convention, *supra* note 197, art. 1.

the DP Convention provides a clearer source for the DP Directive's assertion that individuals have a fundamental right to privacy of PII. Not surprisingly, however, the DP Convention also does not explain how the Council of Europe determined that there is such a fundamental right or what its scope might be. Indeed, if the Council of Europe were a court, one would say that the assertion of a fundamental right to privacy of PII is *ipse dixit*. There is such a fundamental right because the Council of Europe says there is, and in case we are still not convinced, EU legislators repeat the Council of Europe's assertion several times in the DP Directive.

Alasdair MacIntyre has argued that "there are no [human or natural] rights, and belief in them is one with belief in witches and in unicorns."[199] Recognizing that he might be accused of making a very controversial point rather "bluntly," he indicates that "best reason" for concluding that there are no human or natural rights is that "every attempt to give good reasons for believing that there *are* such rights has failed."[200] It is beyond the scope of this article to evaluate MacIntyre's arguments[201] for this claim.[202] His position is, however, consistent with a central tenet of the post-Enlightenment paradigm, i.e., that neither the old teleological paradigm nor its proposed Enlightenment successors such as Kantianism and utilitarianism provides us with a true and adequate theory of human nature and moral life. Thus, assuming claims about natural or fundamental rights are essentially moral claims, it follows that we lack a true theory to support them.[203] Accordingly, under the post-Enlightenment paradigm, such rights claims are rooted in and will reflect each individual's private values.

The view that rights claims stem from private values does not entail the conclusion that such claims serve no purpose. MacIntyre characterizes them as "moral fictions,"[204] and he draws attention to two purposes that they serve. The first is to reinforce the post-Enlightenment paradigm's tenet that the social world consists of individuals interacting and competing with one another. Such individuals are understood as bearers of rights,[205] and in this respect the DP Directive's repeated references to fundamental rights are simply the flip side of the Directive's stress on privacy as a characteristic—a "right" —of the individual. According to MacIntyre:

> [t]he arrival upon the social scene of conceptions of right, attaching to and exercised by individuals, as a fundamental moral quasilegal concept . . . always signals some measure of loss of or repudiation of some previous

---

[199] MACINTYRE, AFTER VIRTUE, *supra* note 12, at 69.

[200] *Id.* (emphasis in original).

[201] For MacIntyre's key arguments, *see id.* at 66–71.

[202] For an interesting discussion of the critical literature on rights discourse covering theorists from Leo Strauss to MacIntyre, John Rawls and Ronald Dworkin, see Thomas J. L Haskell, *The Curious Persistence of Rights Talk in the 'Age of Interpretation,'* 74 J. AM. HIST. 984 (1987).

[203] As Professor Haskell notes, "talk [about rights] implies something highly controversial: the existence of an objective moral order accessible to reason. To be conscious of a right is at least tacitly to lay claim to a kind of knowledge that is not merely personal and subjective but impersonal and objective." *Id.* at 984. Although Haskell appears to concede the epistemological premise of MacIntyre's argument, he criticizes MacIntyre's conclusion, *id.* at 1001–1002, and unlike MacIntyre he appears to be satisfied with a theory of rights that is "without deep epistemological foundations" in which rights are "conventional and historical in character." *Id.* at 1008.

[204] MACINTYRE, AFTER VIRTUE, *supra* note 12, at 70.

[205] *See* Kightlinger, *supra* note 7, at 361.

> social solidarity. Rights are claimed against some other person or persons; they are invoked when and insofar as those others appear as threats.[206]

One ordinarily would not say, for example, that my hypothetical boyfriend and I have rights against one another with respect to use of intimate information that we share about one another,[207] but one typically would say that each of us has a right to protection against a website operator who threatens to misuse that same information. The claim that I have a right against threats by a third party reinforces my understanding of myself as the sort of entity that can possess such rights, i.e., an individual.

The second purpose that moral fictions such as claims about fundamental rights serve is rhetorical. They are, according to MacIntyre, a form of utterance through which people express indignation at and protest against alleged wrongs.[208] Claims about rights provide an apparently neutral theoretical language that "serves to conceal behind the masks of morality what are in fact the preferences of arbitrary will and desire."[209] Thus, for example, when A says "every person has a right to privacy," in practice A typically means that A wants to charge B a higher price for PII; or A wants B to collect, use, and transfer PII only in specified ways and at B's expense; or A wants C, a public official, to interfere with B's collection and use of A's PII. A couches her personal wishes or desires in the language of rights because that language seems to provide a moral reason for giving A what she wishes or desires—she has a right to it. MacIntyre describes as "moral" such fictions as fundamental rights precisely because they allow us to believe or pretend that we are engaging in a reasoned moral discussion rather than a shouting match about who took what from whom or who wants what from whom.

The shouting match and the endless struggle over who gets what are central elements of our actual situation as interpreted by the post-Enlightenment paradigm. Our moral beliefs are said to stem from private values lying beyond rational dispute, but not beyond vehement disagreement. Thus, there is a constant potential for conflict between individuals viewed as holders of private, potentially irreconcilable values. Dressing up claims about values as assertions about "fundamental rights" may serve to mask the irresolvable nature of the underlying conflict at least for those such as EU legislators who apparently claim to know which statements about private values really are assertions about rights and which of those rights really are fundamental. Such masking may in turn help to prevent the dissolution of the social fabric into Hobbesian anarchy.[210] Assuming for the sake of argument that there is merit to this account of the function of discourse about rights under the post-

---

[206] MACINTYRE, THREE RIVAL VERSIONS, *supra* note 12, at 184–85 (emphasis in original).

[207] Rather than characterizing boyfriends as having rights against one another, a more plausible approach would be to say that one characteristic of a good boyfriend is that he displays the virtues of discretion and respect in his use of intimate PII and thus deserves to be trusted with it.

[208] MACINTYRE, AFTER VIRTUE, *supra* note 12, at 71.

[209] *Id.*

[210] For a further application of this line of argument to the EU's information-privacy regime, see *infra* notes 284–88 and accompanying text.

Enlightenment paradigm,[211] it follows that the steady drumbeat of references in the DP Directive to the fundamental right to privacy can be understood as, among other things, an example of post-Enlightenment rhetoric asserting that an undefined "we" vehemently, if arbitrarily, will and desire restrictions on collection and use of PII. The issue of who this "we" is will be taken up in Part IV.C.2, where it will be argued that the rhetoric of fundamental rights, which purports to support and protect the individual's "private life," also in fact supports the authority of bureaucracies to administer and oversee most significant decisions affecting the individual's PII.

Competing with the rhetoric in the DP Directive about protecting fundamental privacy rights are numerous references to the objective of establishing and maintaining an "internal market" in which PII can circulate freely around the European Community. EU legislators adopted the Directive[212] under Article 100a (now Article 95) of the Treaty Establishing the European Community (EC Treaty), which calls for adoption of "measures for the approximation of the provisions laid down by law, regulation or administrative action in Member States which have as their object the establishment and functioning of the internal market."[213] According to the EC Treaty, the "internal market [is] characterized by the abolition, as between Member States, of obstacles to the free movement of goods, persons, services and capital."[214] Thus, EU legislators viewed the Directive as one of many pieces of legislation designed to eliminate barriers to commerce in all forms between and among the Member States.[215] In the language of the Directive, "the establishment and functioning of an internal market . . . require . . . that personal data should be able to flow freely from one Member State to another."[216]

The concern that EU legislators expressed about interference with the free flow of PII in the EU market was not speculative. It arose at least in part because the

---

[211] A proponent of the fundamental right to privacy could, of course, dispute the intellectual underpinnings of the post-Enlightenment paradigm. She first would have to revive and repair either the older teleological paradigm or one of the Enlightenment's proposed replacements, e.g., Kantian moral theory or utilitarianism. She then would have to show that the revived and repaired moral theory entails the conclusion that there is a fundamental right to privacy. Both efforts presumably confront significant hurdles since, if MacIntyre is correct, people have pursued them for hundreds of years without success. The point, however, is not that such efforts are doomed to fail but that we are under no obligation to presume that they will succeed. Rather, it seems reasonable to treat claims about fundamental rights skeptically and to focus on their rhetorical function, which they presumably retain whether or not they have a sound foundation in moral theory. For some concluding comments on these issues, see *infra* Part VI.

[212] DP Directive, *supra* note 42 ("Having regard to the Treaty establishing the European Community, and in particular Article 100a thereof . . .").

[213] Treaty Establishing the European Community (Nice Consolidated Version), Dec. 24, 2002, 2002 O.J. (C 325) 33 art. 95(1) [hereinafter EC Treaty]. Article 100a was renumbered Article 95 by the Treaty of Amsterdam. Treaty of Amsterdam Amending the Treaty on European Union, the Treaties Establishing the European Communities and Certain Related Acts, Oct. 2, 1997, 1997 O.J. (C 340) 173, art. 95.

[214] EC Treaty, *supra* note 213, art. 3(1)(c). For a brief discussion of the rationale for the "internal market," see GEORGE A. BERMANN ET AL., CASES AND MATERIALS ON EUROPEAN UNION LAW 10, 13, 14 (2d ed. 2002). For a more detailed discussion of the internal market, see P.S.R.F. MATHIJSEN, A GUIDE TO EUROPEAN UNION LAW 171–224 (8th ed. 2004).

[215] *See* BERMANN, *supra* note 214, at 14 (listing among the areas in which the EC has adopted internal market legislation "banking, insurance and securities regulation, transport, intellectual property, telecommunications, taxation and public procurement").

[216] DP Directive, *supra* note 42, recital 3.

French national data protection authority[217] had at one point decided to prohibit Fiat's French subsidiary from transferring PII about Fiat's French personnel to Fiat's main office in Italy, thus interfering with Fiat's business operations.[218] The DP Directive does not mention the Fiat matter by name but the Directive clearly was intended to address the type of problem posed by the French decision. As the Directive states:

> the difference in levels of protection of the rights and freedoms of individuals, notably the right to privacy, with regard to the processing of personal data afforded in the Member States may prevent the transmission of such data from the territory of one Member State to that of another Member State; [and] this difference may therefore constitute an obstacle to the pursuit of a number of economic activities at Community level [and] distort competition . . . .[219]

According to the Directive, "in order to remove the obstacles to flows of personal data, the level of protection of the rights and freedoms of individuals with regard to the processing of such data must be equivalent in all Member States . . . [and European] Community action to approximate those laws is therefore needed."[220] Once the Community "approximates" national laws by requiring each Member State to implement the Directive, those laws will provide "equivalent protection . . . [and] Member States will no longer be able to inhibit the free movement between them of personal data . . . ."[221] The Directive characterizes the goal of establishing equivalent levels of data protection throughout the EU as "vital to the internal market."[222]

The DP Directive does not simply pay lip service to the need for a functioning market in which PII can flow without legal impediments throughout the EU. Many of the substantive provisions of the Directive appear to reflect the intent to promote and sustain such a market. As discussed at some length in Part III of this Article, the Directive places some control over an individual's PII in the hands of the individual himself or herself by, for example, establishing consent as one of the recognized legal bases for collection and use of PII.[223] Thus, within limits, the individual can consent to trade his or her PII in the market for a price and on terms the individual considers acceptable. Moreover, within limits, the Directive authorizes website operators to collect and use an individual's ordinary PII for the website operator's own business purposes without the individual's consent.[224] Once PII is lawfully collected, a website operator may transfer it throughout the EU's internal market

---

[217] The French national data protection authority, which was created in 1978, is known as the *Commission Nationale de l'Informatique et des Libertés* or CNIL. The CNIL now serves as France's DPSA under the DP Directive. *See generally* DECREE NO. 2005–5309 of Oct. 20, 2005, Journal Officiel de la République Française [J.O.] [Official Gazette of France], Oct. 22, 2005, p. 16769. For information about the CNIL and its current activities, see The CNIL, http://www.cnil.fr/index.php?id=43

[218] Kightlinger, *supra* note 49, at 10–03.

[219] DP Directive, *supra* note 42, recital 7.

[220] *Id.* recital 8.

[221] *Id.* recital 9.

[222] *Id.* recital 8.

[223] *See supra* notes 76–79 and accompanying text.

[224] *See supra* note 85 and accompanying text.

without legal obstacles, assuming all parties comply with the Directive. Under certain conditions, a website operator can even trade or otherwise transfer an individual's PII to a business or other data controller in a non-EU country without the individual's consent.[225] The Directive actively discourages collection, use, and trading of PII in the market for business purposes only if the PII falls into one of the categories deemed sensitive.[226] And as noted above,[227] those categories are defined by law and not by the individual, thus providing businesses with a predictable legal environment in which to collect, use, and trade PII.

One might reply that the DP Directive actually imposes a range of restrictions on the uses that a website operator may make of an individual's PII in the market once the PII has been collected legitimately. As discussed above,[228] the Directive requires all data controllers to (1) obtain a license from, or register with, a DPSA; (2) satisfy various "data quality" requirements; (3) provide a variety of information to the individual whose PII is to be collected; (4) grant the individual rights of access and correction; and (5) adopt security measures to protect PII. These requirements limit trading of PII within the market. Thus, it is misleading to suggest that the Directive promotes the market interests of website operators in collecting, using and trading PII at the expense of the individual's strong desire for privacy.

The difficulty with this reply is that it misses the point. No one would deny that the DP Directive imposes limits on collection, use, and trading of PII within the market. The point, rather, is that the regime presupposes the existence of a market for PII that is integral to the broader internal market and the Directive promotes the operation of that PII market by establishing the ground rules for its operation. The Directive thus makes individuals and their PII available to serve the needs of the market. And as something that can be traded in a market, each item of PII becomes a commodity with a price.[229] The question whether there should be a PII market, however regulated, is not and cannot be raised seriously, because the market is the element of the post-Enlightenment paradigm through which we understand how individuals interact to pursue their objectives as defined by their values.[230] Indeed, under the post-Enlightenment paradigm, it is all but unthinkable that individuals would not be able to trade PII in a market. The PII market is, therefore, a premise of the DP Directive, and just as the PII market is crucial to the internal market, so the Directive that regulates the PII market is "vital to the internal market."[231]

As one would expect under the post-Enlightenment paradigm, which ties individuals firmly to markets in which they pursue their interests, circulation of PII as a commodity is vital not only to the EU's internal market but also to the individual. This is because the individual can acquire an identity in the electronic

---

[225] *See supra* Part III.B.3.

[226] *See supra* Part III.B.2.

[227] *See supra* notes 90–95 and accompanying text.

[228] *See supra* Part III.C.

[229] *See* Kightlinger, *supra* note 7, at 385. For a brief discussion of the distinctive features of information as a form of property that parties can trade, see MANN & WINN, *supra* note 3, at 380–81.

[230] *See* Kightlinger, *supra* note 7, at 386–88 (showing that the U.S. Internet privacy regime both presumes a market for PII and promotes the operation of that market).

[231] *See supra* note 222 and accompanying text.

market, an identity as this particular individual, only by trading his or her PII. To participate in a market transaction at a distance, the individual must be willing and able to identify himself or herself to a counterparty who otherwise would not know with whom he/she/it is dealing. The individual does this by supplying PII to the counterparty. If I do not provide such information as a name, street address, email address, and credit card number, Amazon.UK cannot know that I am the particular individual who wants to buy the latest Paul Russell novel and Amazon.UK presumably cannot and will not sell it to me. In general, if I refuse to trade my PII within the market, I will lose my identity in the market.[232] I will render myself indistinguishable from other individuals and thus cease to be a distinct individual—at least from the market's perspective. Seen in this light, the DP Directive provides a legal framework within which individuals can disseminate PII to establish their identities in the market, and the market that circulates PII among individuals and organizations plays an essential role in the establishment of individual identity—as one would expect under the post-Enlightenment paradigm.

It should now be clear in what sense the DP Directive reflects the basic ambivalence toward PII and its privacy that is a hallmark of the post-Enlightenment paradigm. A premise of the Directive is that individuals place, or should place, a high value on the privacy of PII, and the Directive rhetorically endorses this evaluation by declaring that the privacy of PII is a fundamental right. At the same time, the Directive facilitates trading of PII by presupposing and promoting a market for PII. The Directive seeks to protect the privacy of PII that defines who I am as this individual by enabling me to trade that PII as a commodity. In exchange for my PII and other items that I value, I can obtain other commodities in the market that I value more.

The DP Directive's ambivalence toward PII and its privacy has roots in the Directive's treatment of personal identity. In the Directive's parlance, I am a "data subject."[233] But who or what exactly is a data subject? One plausible approach to that question would be to list those items of PII or personal data that are predicates of the subject. But the predicates that one typically would list—i.e., name, sex, age, height, weight, and so forth—are not essential to the data subject qua data subject because they will differ from subject to subject and in many instances from time to time with respect to particular subjects. That which subsists through these predicates, the identity of the "I" that is the underlying data subject, seems to escape such predication and thus in an important sense lies beyond description. Perhaps what can be said of the data subject is that it is a continuing potential to gather predicates together into an individual. Beyond that continuing potential, the data

[232] Researchers continue to develop technologies that may facilitate online trading without requiring parties to exchange such sensitive PII as credit card information. *See* Joris Evers, *IBM Donates New Privacy Tool to Open-Source*, *available at* http://news.com.com /2100–0029_3–3153625.html. Currently, such technologies allow a trusted third party such as a credit card company to hold the sensitive information and operate as a go-between for the parties. *Id.* Such trusted-third-party systems presume, of course, that the individual is willing to supply PII to the third party. Thus, the individual still must surrender PII to someone in the market in order for an electronic transaction to unfold.

[233] *See supra* note 53 and accompanying text.

subject arguably is nothing at all and it vanishes into the realm of silence, the realm of that about which nothing more can be said.

The data subject that appears in the DP Directive accurately reflects certain distinctively modern accounts of personal identity or the individual self that emerge under the post-Enlightenment paradigm.[234] As MacIntyre has written, this "self which has no necessary social content and no necessary social identity can . . . be anything, can assume any role or take any point of view, because it *is* in and for itself nothing."[235] The data subject that is in and for itself nothing is the "I" that or whom the Directive protects. To this "I" who is nothing, PII is at once inessential and necessary. PII tells us nothing about the underlying data subject and therefore is inessential. It can be alienated, acquired, and changed like a suit of clothes. I can treat it as a commodity and sell it to the highest bidder or on the best terms. On the other hand, without my PII, I am little more than a continuing potential to be something, and this is tantamount to being nothing.[236] Any threat to my PII is a threat to what distinguishes me from all other data subjects and thus to my identity. Hence, I am likely to be deeply concerned about such threats. My strong desire to protect my PII against such threats finds voice in the assertion of a fundamental right to information privacy. Ambivalence to PII is thus built into the structure of the relationship between the data subject—the "I" —and his or her PII.

One might respond—reasonably—that the DP Directive is simply a law and so it is unfair to elicit from the Directive a philosophy of identity or the human self. But it is a thesis of this Article that the Directive reflects and reinforces a particular type of philosophy, or more accurately, a particular paradigmatic way of seeing human nature and moral life that is characteristic of our modern condition. Seen from this perspective, it is not an accident that the Directive treats the human self as a numinous, vanishing individual data subject that fears to lose PII and yet needs to trade PII as a commodity in the market. Policy pronouncements by the DPSA Working Party tend to confirm this account of the Directive's approach to personal identity. The DPSAs have argued that a person should be able to use an electronic market anonymously, just as a person may purchase anonymously from the "vendor in a small corner shop [who] is not interested in the identity of his customer . . . ."[237] According to the DPSAs, "the possibility of remaining anonymous is essential if the fundamental rights to privacy and freedom of expression are to be maintained in cyberspace."[238] Thus, for the DPSAs, anonymity represents a desirable policy goal and perhaps even an ideal form of personal privacy, at least on the internet. This suggests, however, that for the DPSAs, personal privacy may be equivalent in certain circumstances to namelessness or even identitylessness, since mere namelessness

---

[234] *See* MACINTYRE, AFTER VIRTUE, *supra* note 12, at 32 (discussing the parallels between the accounts of the individual self offered by Jean-Paul Sartre and Irving Goffmann) and 115–17 (discussing the parallels between the accounts offered by Goffmann and Friedrich Nietzsche).

[235] *Id.* at 32.

[236] *See* Kightlinger, *supra* note 7, at 364–65 (discussing the anxiety that the individual would be likely to feel with loss of control over PII).

[237] *See* DPSA Working Party, Recommendation 3/97, Anonymity on the Internet, XV D /5022/97 Final (Dec. 3, 1997), *available at* http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/1997/wp6_en.pdf.

[238] *Id.* at 5.

may not suffice to preserve anonymity in the electronic environment. Thus, an ideal form of privacy for me would be to enter the electronic market without my PII as a naked data subject, a naked "I," the primary characteristic of which is that it is someone or something about whom/which nothing personal can be said. This in turn seems to imply that, according to the DPSA Working Party, my fundamental right to privacy includes a right to be no one. As no one in particular, I could be anyone. To paraphrase MacIntyre, I could assume any role or point of view, because, as an anonymous data subject, I am in essence nothing. Through discussions such as this one of anonymity as a policy goal, the DPSA Working Party shows that the Directive reflects the rudiments of a philosophy of personal identity or the individual self rooted in the post-Enlightenment paradigm.

If further evidence of the DP Directive's ambivalence to PII and its privacy were required, one need look no further than the Directive's treatment of PII in the "purely personal" space. As discussed above,[239] the Directive recognizes but does not regulate a space for purely personal activity in which people hold and use PII about one another and their relationships. Such PII is not treated as "personal data" regulated by the Directive and therefore is not subject to individual consensual control. Assuming the Directive adequately defines or formalizes the scope of the fundamental right to information privacy, it would appear to follow that the Directive, by excluding PII in the purely personal space, signals that the fundamental right does not cover such PII. Not surprisingly, this inference is consistent with the post-Enlightenment paradigm's account of the individual as a bearer of rights.[240] The person within the purely personal space is not presumed to be an individual under the Directive and therefore would not be a bearer of rights, including the right to information privacy. Moreover, assuming rights claims are a form of rhetoric, if the Directive's assertion of a right to information privacy signals a strongly held desire to protect PII, then the Directive's exclusion of PII in the purely personal space suggests that the desire to protect PII does not extend to PII in the purely personal space. One might say that the more personal and intimate the information, the less its significance from the perspective of the Directive. PII becomes legally significant and a fit subject of fundamental rights only when it leaves the purely personal space and enters the market.

These remarks about the purely personal space recognized by the DP Directive pose a challenge to the post-Enlightenment paradigm. Insofar as a person acts within the purely personal space, holding PII about family, friends, lovers, and so forth, the person apparently does not come into contact with the PII market. By trading PII on the market, the person crosses the boundary line demarcating the purely personal space. This means, however, that the Directive presumes that relations between people within the purely personal space are not market relations. Insofar as a relationship in the purely personal space evolves into a market relationship, it apparently would drop out of the purely personal space and become subject to the Directive. As discussed above,[241] the post-Enlightenment paradigm

[239] *See supra* note 184 and accompanying text.
[240] *See supra* notes 204–06 and accompanying text.
[241] *See supra* notes 24–26 and accompanying text..

seeks to explain and justify human action by reference to markets in which each person, understood to be an individual, pursues his or her own interests according to his or her own values. The post-Enlightenment paradigm cannot adequately explain and justify actions within the purely personal space via the analytical construct of the market because by hypothesis the purely personal space comprises such non-market relationships as family, friendship, and love. Yet the Directive appears to presume that PII will be safe within such relationships despite the absence of legal protection for fundamental rights. To explain such intimate relationships and justify treating PII as safe within them appears to require an alternative paradigm that does not rely on the notion of rights-bearing individuals trading in markets. Developing such an alternative is beyond the scope of this Article, but again it is worth noting that exponents of the old Aristotelian paradigm offered alternative accounts of the trusting relationship of people within a family that did not involve reference to a market.[242]

C. *Impersonality, Bureaucracy, and the Administration of Privacy*

In Part II, this Article explained that the U.S. internet privacy regime, following the post-Enlightenment paradigm, relies heavily on administrative bureaucracy to counter the potential chaos of individual wills expressed in the market in the absence of a shared vision of the good.[243] Heavy reliance on bureaucracy is, not surprisingly, a defining characteristic of the culture of bureaucratic individualism. As shown in this Part, bureaucracy plays the same paradigmatic role under the EU internet privacy regime. The persuasiveness of this claim depends on, among other things, what one means by the term "bureaucracy." The appropriate starting point for a discussion of bureaucratic organization is the work of Max Weber.[244] According to Talcott Parsons, for Weber a bureaucracy is

> an organization devoted to what is from the point of view of the participants an impersonal end. It is based on a type of division of labor which involves specialization in terms of clearly differentiated functions, divided according to technical criteria, with a corresponding division of authority hierarchically organized, heading up to a central organ, and specialized technical qualifications on the part of the participants. The role of each participant is conceived of as an "office" where he acts by

---

[242] For Aristotle's discussion of the family, see ARISTOTLE, POLITICS 18–89 (Ernest Barker trans., 1948). For a later discussion along the same lines, see GEORG WILHELM FRIEDRICH HEGEL, HEGEL'S PHILOSOPHY OF RIGHT 110 (T. M. Knox trans., Oxford Univ. Press 1967) (1821).

[243] *See supra* Part II.

[244] MacIntyre has stated that his account of the role of bureaucracy is indebted to the work of Weber. MACINTYRE, AFTER VIRTUE, *supra* note 12, at 86, 109. In the words of Professor Gorski, "[e]ven today, Weber's definition [of bureaucracy] still serves as the starting point for most work on the subject." Philip S. Gorski, *The Protestant Ethic and the Bureaucratic Revolution: Ascetic Protestantism and Administrative Rationalization in Early Modern Europe*, *in* MAX WEBER'S *ECONOMY AND SOCIETY*: A CRITICAL COMPANION 267, 267 (Charles Camic et al. eds., 2005). In a similar vein, after identifying a number of weaknesses in Weber's analysis of authority, including his account of bureaucracy, Talcott Parsons concluded "[p]robably Weber's analysis of authority even as it stands constitutes the most highly developed and broadly applicable conceptual scheme in any comparable field which is available, not only in the specifically sociological literature, but in that of social science as a whole." *Introduction* to MAX WEBER, THE THEORY OF SOCIAL AND ECONOMIC ORGANIZATION 77 (Talcott Parsons ed., Oxford Univ. Press 1947).

> virtue of the authority vested in the office and not of his personal influence.[245]

As Weber states, within a bureaucracy, "[i]ndividual performances are allocated to functionaries who have specialized training and who by constant practice increase their expertise. 'Objective' discharge of business primarily means a discharge of business according to *calculable rules* and 'without regard for persons.'"[246] As a result of detailed studies of authority structures in various periods of human history,[247] Weber concluded that bureaucracy in the sense described has become the paradigmatic modern structure of authority and power in both the private and public sectors.[248] Thus, assuming Weber is broadly correct,[249] it would be surprising if a law such as the DP Directive, which relies heavily on administrative oversight, did not equate administration with impersonal, hierarchically organized, technically specialized bureaucracy.

As discussed in the following parts, the DP Directive reflects and reinforces the culture of bureaucratic (in Weber's sense) individualism in at least two respects. First, under the Directive, the bureaucratic structures that run modern business organizations channel and coordinate potentially chaotic values that different individuals assign to their interests and objectives, including the privacy of their PII, into a relatively orderly system.[250] Second, and more importantly in the EU context, the Directive establishes public bureaucracies—i.e., the DPSAs—to administer the operation of the PII market, set many of the terms according to which a website operator may collect and use PII, and thereby lessen the threat of conflict and chaos that arises when individuals and business organizations deal with one another directly.[251] In each of these respects, under the Directive, the impersonal bureaucracy proves to be a necessary condition for the protection of PII that constitutes the personal identity of the individual. Calls for protection of the individual's fundamental right to privacy function as justifications for the expansion of bureaucratic control and authority. The DP Directive thus clearly reflects and reinforces the culture of bureaucratic individualism that lies at the core of the post-Enlightenment paradigm.

---

[245] TALCOTT PARSONS, THE STRUCTURE OF SOCIAL ACTION 506 (2d ed. 1949).

[246] MAX WEBER, ECONOMY AND SOCIETY 975 (Guenther Roth & Claus Wittich eds., 1968) (emphasis in original).

[247] For one of Weber's discussions of his research in this area, see *id.* at 212–301.

[248] *See id.* at 223. For a summary of Weber's views on the importance of bureaucracy in a modern economy, see ANTHONY GIDDENS, CAPITALISM AND MODERN SOCIAL THEORY: AN ANALYSIS OF THE WRITINGS OF MARX, DURKHEIM AND MAX WEBER 158–60 (1971).

[249] While recognizing the central importance of Weber's work, MacIntyre has noted that "Weber's account of bureaucracy notoriously has many flaws." MACINTYRE, AFTER VIRTUE, *supra* note 12, at 86. For critical comments on Weber, see ALASDAIR MACINTYRE, *Social Science Methodology as the Ideology of Bureaucratic Authority*, *in* THE MACINTYRE READER 53, 64–67 (Kelvin Knight ed., 1998). For more biting criticisms, see Rodney Stark, *SSSR Presidential Address, 2004: Putting an End to Ancestor Worship*, 43 J. SCI. STUD. OF REL. 465, 465–68 (2004). A critical examination of the extensive literature on Weber is beyond the scope of this Article.

[250] *See infra* Part IV.C.1.

[251] *See infra* Part IV.C.2.

1. Privacy and the Bureaucratic Business Organization

Given the importance of the DPSAs and, therefore, of public bureaucracies in the operation of the DP Directive, it would be easy to overlook the fact that the bureaucracies with which individuals ordinarily deal in the market for PII are those that run businesses such as commercial websites.[252] There are two important pieces of evidence indicating that the EU legislators who adopted the DP Directive expected that such businesses would be bureaucratically organized. First, the term "data controller" may be used to refer not only to a business organization as a whole that controls items of PII but also to the person or people within the organization who determine(s) the purposes and means for collecting and using PII.[253] In this sense, the term "data controller" denotes an office within an organization, an office that the Directive presumes will ordinarily stand below the offices of the people who run the organization but above the offices of people who actually collect and/or use PII on the organization's behalf. The officeholders below the data controller(s) are expected to follow any instructions issued by the data controller(s), just as the data controller(s) must seek to implement the business objectives defined by superior officials, if any, within the bureaucratic hierarchy.[254]

Second, as discussed briefly above,[255] the DP Directive grants an organization the legal right to establish a special office—that of the "data protection official"—within its bureaucratic hierarchy. Among other things, a data protection official will be responsible "for ensuring in an independent manner the internal application of the national provisions taken pursuant to th[e] Directive."[256] Thus, in an organization that elects to establish the office of "data protection official," the office—note the Weberian language—should have at least some authority over all other offices within the organization that collect and use PII, presumably including the office of data controller. The Directive reinforces this requirement by stating that "a data protection official, whether or not an employee of the controller, must be in a position to exercise his functions in complete independence."[257] Thus, whatever the data protection official's nominal position within the bureaucratic hierarchy, the data protection official must be able to carry out the distinctive responsibilities of his or her office independently of any commands that may originate at higher levels of the bureaucracy. One might say that the official is required to stand at the apex of a particular section of the bureaucracy overseeing the legality of all collection and use of PII. Again, the Directive clearly presumes that other officials within the bureaucratic hierarchy will, or at least should, do their bureaucratic duty and carry

[252] According to Talcott Parsons, for Weber the "principal distinguishing feature of the modern Western economic order" is "'bureaucratic organization' in the service of pecuniary profit in a system of market relations." PARSONS, *supra* note 245, at 508.

[253] *See supra* note 51 and accompanying text.

[254] In some organizations, the highest-ranking officials presumably are the data controller(s) because those officials determine the purpose of and means for data collection and use.

[255] *See supra* note 132 and accompanying text.

[256] DP Directive, *supra* note 42, art. 18(2).

[257] *Id.* recital 49.

out the data protection official's instructions.[258] In light of the DP Directive's treatment of the offices of data controller and data protection official, it seems clear that EU legislators presumed that a website operator or other organization collecting and using PII ordinarily would be set up as a hierarchical structure of specialized offices, i.e., a bureaucracy.

Under the post-Enlightenment paradigm, the bureaucratically organized website operator plays a crucial role in the electronic market for PII.[259] According to the paradigm, each individual will assign a value to his or her PII within the market. One factor in the individual's evaluation presumably will be his or her privacy preferences. Multiple, conflicting individual values could lead to a situation in which there are as many different market values for an item or collection of PII as there are individuals operating within the market. Consequently, the market for PII would be confusing and potentially chaotic, perhaps discouraging some people from trading and obtaining an acceptable value for their PII. In dealing with individual consumers, a bureaucratically organized website operator such as Amazon.UK will channel and coordinate these individual values into a more or less uniform price structure for PII, a common set of terms and conditions under which all interested individuals submit PII to Amazon.UK in exchange for goods, services, and other benefits.[260] For its part, Amazon.UK will collect and use the individual's PII to further Amazon.UK's organizational interests, which might include increasing sales, profits, market share, share value, and so forth.

Amazon.UK does not, of course, have an entirely free hand in setting the price for PII. Amazon.UK has to compete in the market for PII with other website operators pursuing their organizational interests. Over time, one might expect Amazon.UK and comparable website operators to offer relatively similar prices and terms for PII, thereby further channeling and coordinating the welter of individual values into an orderly market with relatively uniform prices and other terms. Thus, as the post-Enlightenment paradigm requires, bureaucratic business organizations operating through the market tend to counteract the chaos that appears to be inevitable when individuals pursue individual objectives according to individual values without a shared vision of the good. The DP Directive reinforces this arrangement by providing legal support for individual consent within the market while at the same time expressly authorizing bureaucratic business organizations such as website operators to collect and use PII for their own purposes. It should be emphasized that the point here is not to denigrate the role of bureaucratically organized website operators in the PII market. It is hardly a criticism to say that Amazon.UK collects and uses PII in Amazon.UK's interests. Why else would Amazon.UK collect and use PII? The point is rather to identify the crucial role of

---

[258] As Reinhard Bendix wrote, "[t]he ideal official . . . must put his sense of duty above his personal opinion, and his ability to do this well is ideally part of his professional ethic." REINHARD BENDIX, MAX WEBER: AN INTELLECTUAL PORTRAIT 440 (1977).

[259] *See* Kightlinger, *supra* note 7, at 403–05 (discussing the role of the bureaucratically organized website operator under U.S. privacy law).

[260] For the current version of the privacy policy on Amazon's United Kingdom website, see http://www.amazon.co.uk/ (follow "HELP" hyperlink; then follow "Privacy Notice" hyperlink) (last visited March 20, 2007).

the business organizational bureaucracy under the DP Directive as an institution that channels and coordinates individual values within the PII market.

If Reinhardt Bendix is correct that for Weber bureaucratic "organizations operate more efficiently than alternative systems of administration and . . . they increase their efficiency to the extent that they 'depersonalize' the execution of official tasks,"[261] then one would expect a bureaucratic business organization to depersonalize tasks related to collection and use of PII. The organization would, in other words, seek to adopt an impersonal approach to personal information. Using (or misusing) someone's PII for personal reasons would violate the bureaucratic principle of depersonalization. So, for example, if Amazon.UK collects the information that I like to read gay-themed novels, Amazon.UK does so not because it or its employees have a prurient or malign interest in my sexual orientation but because collecting such information will help Amazon.UK to achieve its impersonal organizational goals.[262] Amazon.UK can, for example, use my PII to target me with announcements about the publication of new gay-themed novels, and thereby solicit new orders. Thus, Amazon.UK's use of my PII reflects a business interest and not a personal interest on the part of the organization or its officials. Modern data processing technology actually assists in depersonalizing bureaucratic control over PII by removing human beings and their personal interests from most aspects of data collection and use, particularly in the field of electronic commerce.[263] In theory, the only person at Amazon.UK who needs to know anything about me might be the one who packs my books in a box bearing my name and address.

The DP Directive reinforces the bureaucratic principle of depersonalization, stating that "[a]ny person acting under the authority of the controller . . . who has access to personal data must not process them except on instructions from the controller, unless he is required to do so by law."[264] Thus, the data controller within an organization dictates the organization's official reasons and rules for collecting and using PII. Every company official involved in such collection and use is bureaucratically subordinate to the data controller and by law must adhere to the data controller's instructions, eschewing any unofficial (read: personal) interest in PII or its use. The Directive thus presumes and reinforces a system in which, ideally, the impersonal business bureaucracy wields impersonal data processing technology to collect and use PII and thereby channels and coordinates the personal and private values and objectives of individuals in the market to further the business's interests. Without the activities of the impersonal bureaucracy, chaos might result, according to the post-Enlightenment paradigm.

---

[261] BENDIX, *supra* note 258, at 427. For a discussion of the relative strengths of bureaucratic organizational structures over historical alternatives, see *id.* at 426–30.

[262] These organizational goals would include the business purposes that the DP Directive recognizes, within limits, as a legitimate basis for collecting and using PII, even without the individual's consent. *See supra* notes 85–87 and accompanying text.

[263] Kightlinger, *supra* note 7, at 404.

[264] DP Directive, *supra* note 42, art. 16.

2. Privacy and Public Administration

In the preceding Part, the discussion focused on the significant role of private bureaucratic organizations under the EU internet privacy regime and showed how that role is what one would expect in a world that reflects the post-Enlightenment paradigm. This initial focus on private bureaucratic organizations resulted in part from the fact that their role easily might be overlooked in a discussion of the EU regime. There is, however, another set of bureaucratic organizations established by the EU regime that it would be very difficult to overlook, namely the DPSAs. These organizations are tasked with administering the national laws implementing the DP Directive in their respective Member States.[265] One of the main arguments of this Article has been that DPSAs play a central role, if not the central role, in the operation of the EU regime and no further effort will be made here to demonstrate that point. Rather, the purpose of the following discussion is to explore the significance under the post-Enlightenment paradigm of the role that the DPSAs play.

As Alasdair MacIntyre argues, a principal function of the bureaucracy within the culture of bureaucratic individualism is to "limit the free and arbitrary choices of individuals."[266] The need for an institution that so limits individual choice arises from the ever-present threat of disorder and chaos in a world where individual values drive individual actions in the absence of a shared vision of the good. Based on the discussion in Part IV.C.1, however, it would seem that bureaucratically structured business organizations operating in a market may limit individual choice sufficiently to eliminate or at least considerably reduce the threat of disorder and chaos. As a result, there should be no need for a further layer of bureaucracy to oversee the operation of the market. Yet it is absolutely clear that in the EU and other advanced industrial regions and countries, one or more layers of public bureaucratic administration do oversee the operation of most, if not all, markets and fields of individual activity.[267] In this respect, the decision to establish the DPSAs represents a normal response by EU legislators to the emergence of the new market for PII.

Theorists of administrative law in the United States have attempted to explain the connection between markets and public administrative bureaucracies by noting that markets are presumed to malfunction. According to Professor Rabin,[268] it is possible to sort administrative agencies among different models depending upon the type of presumed market malfunction that the agency was intended to address. For purposes of this Article, two such models are relevant. The first, known as the "policing model," was intended to respond to "certain 'excessively competitive' [market] practices such as the manufacture of products that seriously endangered

---

[265] *See supra* note 57 and accompanying text.

[266] *See supra* note 32 and accompanying text.

[267] There are, for example, more than 20 highly bureaucratic Directorates General in the European Commission overseeing the operations of such diverse markets and fields as agriculture and rural development, fisheries and maritime affairs, and transport and energy. For a current list of the Commission's Policy Directorates General and Services, see European Commission Directorates-General and Services, http://ec.europa.eu/dgs_en.htm.

[268] Robert L. Rabin, *Federal Regulation in Historical Perspective*, 38 STAN. L. REV. 1189 (1986). For a more detailed summary and discussion of Rabin's argument, see Kightlinger, *supra* note 7, at 377–83.

health and safety or the setting of rates that were particularly discriminatory."[269] The agency's task under the policing model is to intervene in the market as necessary to police such excessively competitive practices and thus deter them. When such practices are deterred, the policing model presumes that the market will function properly without further administrative intervention. In an earlier article on the U.S. internet privacy regime, I argued that the FTC's approach to administering the market for PII follows the policing model.[270] In effect, the FTC identified as excessively competitive the practice of making false or misleading statements about the extent of privacy protection on websites that collect PII. The FTC then took on the task of deterring this practice, thereby promoting the trading of PII within what is presumed to be a properly functioning market in which an individual can sell PII for an appropriate price based on accurate information.

According to Rabin, in contrast to the policing model the "market-corrective model" presumes that orderly markets require a "commitment to permanent market stabilization activity by the . . . government."[271] Occasional intervention as foreseen by the policing model will not suffice. In the United States, particularly during the New Deal era, an agency following the market-corrective model typically engaged in "price-fixing, information-sharing and market-allocating schemes . . . ."[272] Government assumed substantial responsibility for economic planning because, as Professor Gifford remarked, "planning and supervision of growth are logical outcomes of price and entry regulation."[273] The market-corrective model thus presumes that even after all excessively competitive practices, including false and misleading statements, unsafe products, and predatory pricing, have been deterred, the market nevertheless will tend to produce unacceptable outcomes, perhaps because of unequal bargaining power or for other reasons.[274] From the standpoint of the market-corrective model, the market will continue to be unstable and disorderly without constant administrative supervision.[275] In this respect, the market-corrective model reflects with even greater precision than the policing model the post-Enlightenment paradigm's account of the need for public administrative bureaucracies in the culture of bureaucratic individualism. Such bureaucracies provide continuous assurance of order and stability in a potentially chaotic world of individuals pursuing their own interests according to their own values.

Implicit in this discussion of the policing and market-corrective models is an answer to the argument that private bureaucratic organizations such as website operators could provide the order and stability that the post-Enlightenment paradigm demands in a potentially chaotic world of individuals pursuing individual interests.

---

[269] Rabin, *supra* note 268, at 1192.

[270] *See* Kightlinger, *supra* note 7, at 383–94.

[271] *See* Rabin, *supra* note 268, at 1192.

[272] *Id.* at 1192.

[273] Daniel J. Gifford, *The New Deal Regulatory Model: A History of Criticisms and Refinements*, 68 MINN. L. REV. 299, 303 (1983).

[274] *See* Rabin, *supra* note 268, at 1253 (market-corrective National Labor Relations Act "served as a buffer against inequality of bargaining power in the labor market").

[275] For an example of this kind of reasoning, see Nat'l Broadcasting Co. v. U.S., 319 U.S. 190, 210–218 (1943) (discussing the crucial role of the Federal Communications Commission in stabilizing the market for radio frequencies).

Both models appear to treat such private organizations, despite their complex bureaucratic structures, as equivalent to individuals or natural persons competing in the market.[276] The policing model presumes that such organizations may engage in overly aggressive market behavior such as deceptive advertising and thus must be deterred by public bureaucracies such as the FTC.[277] The market-corrective model goes further and presumes that private bureaucratic organizations may produce unacceptable outcomes even when they pursue their interests in a manner that is not overly aggressive, entering into informed, wholly consensual agreements with other organizations and individuals. The market-corrective model posits that a public administrative agency—i.e., a bureaucracy—must continuously oversee such practices as market entry, pricing, information sharing, resource use, and so forth in order to prevent unacceptable outcomes and stave off possible market malfunction. One might say that, although private bureaucratic organizations do help to produce order and stability in markets, from the perspective of the policing and market-corrective models, such organizations nevertheless are part of the problem rather than the solution.

Professor Rabin developed his account of the distinction between the policing model and the market-corrective model to help explain the evolution of administrative law in the United States. There is no reason, however, why his distinction cannot be used to illuminate the role of the DPSA in the PII market under the DP Directive.[278] Assuming that one can apply Rabin's distinction in the EU context, it seems clear that the role of the DPSA goes well beyond mere policing of excessively competitive practices. Indeed, the DP Directive wastes little space identifying prohibited practices that the DPSA might police. Instead, as one would expect under the market-corrective model, the DP Directive controls entry into the market for PII;[279] mandates the sharing of information with regulators and consumers;[280] empowers the DPSA to apply such standards as fairness, adequacy, legitimacy, and relevancy to set or influence the prices and terms according to which PII may be collected;[281] and generally regulates collection, use and trading of PII as a resource or commodity. Moreover, as one would expect under the market-corrective model and as has been shown repeatedly in this Article, the DP Directive limits the legal significance of individual consent, implying that individuals often cannot be trusted to enter into transactions involving their PII because they may agree to arrangements that are unacceptable even though freely entered into and fully informed. To quote the summary of an earlier part of this Article, under the DP

---

[276] Corporate law adopts a similar approach. Corporations generally have legal personality, meaning that for most purposes the law treats them in the same way that it treats living individuals. As Professor Clark wrote, "[f]or legal purposes, a corporation is almost as much an entity as a natural person." ROBERT CHARLES CLARK, CORPORATE LAW 17 (1986).

[277] Not surprisingly, some scholars have argued that the market would deter such behavior without the intervention of the FTC. *See* Richard A. Posner, *The Federal Trade Commission*, 37 U. CHI. L. REV. 47, 61–70 (1969).

[278] *See* Kightlinger, *supra* note 7, at 377–78 (discussing the use of Rabin's models as analytical tools in the U.S. context).

[279] *See supra* Part III.C.1.

[280] *See supra* Part III.C.3

[281] *See supra* notes 139 to 145 and accompanying text.

Directive, "consent is often unnecessary and never sufficient to legitimate collection and use of PII."

At this point in the argument, there would appear to be an obvious response. The reason that consent is never sufficient under the DP Directive, the reason that the Directive empowers the DPSA to intervene broadly in the market, is that EU legislators believed information privacy to be a fundamental right, and they said so repeatedly in the Directive.[282] The market, if left to its own devices or regulated lightly under the policing model, will tolerate and perhaps even encourage modes of PII collection and use that are unacceptable, even if all parties have consented, precisely because those modes violate the fundamental rights of the individuals concerned. The Directive follows the market-corrective model in order to ensure that the PII market receives the type of continuous supervision required to prevent violations of fundamental rights that might occur under the policing model.

It would come as no surprise if EU officials cited the need to protect fundamental rights as a justification for the EU's market-corrective approach.[283] Such a justification would, however, provide further evidence that the EU regime reflects the post-Enlightenment paradigm. As discussed above,[284] Alasdair MacIntyre has argued that assertions about human or fundamental rights are "moral fictions" that mask arbitrary individual preferences, claims, and grievances in an apparently neutral moral language. The preferences, claims, and grievances are arbitrary, according to the post-Enlightenment paradigm, because there is assumed to be no true account of the human good or *telos*, no shared vision of the good, from which one can derive a list of true moral and ethical precepts,[285] including true precepts about natural or fundamental rights. Consistent with MacIntyre's analysis, the moral fiction that there is a fundamental right to information privacy performs at least two important rhetorical functions in the argument justifying the DP Directive's market-corrective approach. First, it asserts the moral superiority of the speaker's position. He or she is articulating and promoting a fundamental right, and thus anyone who questions the broad, market-corrective powers of the DPSA may be accused of undermining fundamental rights. This rhetorical strategy tends to place the moral underpinnings of the DP Directive and the DPSA's mission beyond serious debate. Of course, one of the tenets of the post-Enlightenment paradigm is that such moral claims are in fact beyond reasoned debate and therefore ultimately

---

[282] For a discussion of the evidence supporting this claim, see *supra* notes 194–198 and accompanying text.

[283] The DPSA Working Party often relies on the rhetoric of fundamental rights to justify its views on privacy issues and proper interpretation of the DP Directive. *See, e.g.*, DPSA Working Party, *Strategy Document* 4 (Sept. 29, 2004), *available at* http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2004/wp98_en.pdf; DPSA Working Party, *Opinion 10/2001 on the Need for a Balanced Approach in the Fight Against Terrorism* 3–3 (Dec. 14, 2001), *available at* http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2001/wp53en.pdf; DPSA Working Party, *Recommendation 4/99 on the Inclusion of the Fundamental Right to Data Protection in the European Catalogue of Fundamental Rights* 3 (Sept. 7, 1999), *available at* http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/1999/wp26en.pdf. Thus, it would be standard practice to cite fundamental rights to justify the Directive's reliance on the market-corrective model, and examining this rhetorical move is not discussing a straw man.

[284] *See supra* notes 199–209 and accompanying text.

[285] *See supra* note 21 and accompanying text.

arbitrary. Thus, the rhetorical strategy of invoking a fundamental right in order to cut off further debate also tends to mask the impossibility of further useful debate.[286]

The second rhetorical purpose of the moral fiction that there is a fundamental right to privacy is political in the Weberian sense that it justifies and rationalizes, or at least seeks to justify and rationalize, relationships of power and control based on the threat of force.[287] Specifically, the claim that there is a fundamental right to privacy serves to rationalize and justify the expansion of bureaucratic control over individual and organizational behavior. *Because* there is a fundamental right to privacy, *there must be* a DP Directive that embodies the right *and* a DPSA to apply the Directive to individuals and organizations, with the accompanying threat of force to bring the recalcitrant into compliance. Among the recalcitrant to be threatened are, of course, those individuals and organizations that do not assign a value to privacy protection that is consistent with the value assigned by those who claim that privacy protection is a fundamental right. It is important to note, moreover, that the rhetoric of fundamental rights serves to justify the expansion of bureaucratic control whether the rhetoric is used by a DPSA to defend its own role or by an individual to call for greater protection of privacy. The unspoken implication is that without the powerful, market-corrective DPSA established by the Directive, the individual's presumed right would not be protected, and the privacy of the individual's PII would be threatened by others who presumably do not place the proper value on the individual's privacy.

As one would expect in the culture of bureaucratic individualism, the rhetorical assertion of a fundamental right to privacy reveals the symbiotic relationship between individual and bureaucracy as well as the limits of that relationship. The individual depends upon the bureaucracy to protect the PII that constitutes his or her identity as this individual and the bureaucracy justifies its existence and expanding power by citing the need to protect individuals from themselves and others – and ultimately from the chaos of Hobbes's "warre . . . of every man, against every man."[288] A person can remain outside the symbiotic relationship between individual and bureaucracy only when and insofar as the person holds and uses PII within the purely personal space that lies beyond the scope of the Directive and, by implication, the post-Enlightenment paradigm. Qua participant in the purely personal space, I

---

[286] This argument does not entail, and is not intended to entail, the conclusion that those who make claims about the fundamental right to privacy are intentionally propagating moral fictions or intentionally masking arbitrary preferences. Indeed, I suspect that many if not most of the people who make claims about the fundamental right to privacy do not have a hidden agenda. I also suspect, however, that if drawn into a serious moral dispute about fundamental convictions, many of these same people would fall back on a version of the argument that all moral precepts reflect the private values of the individuals who hold those precepts and that those precepts therefore lie irretrievably beyond rational debate. How those same people would square the latter position on the foundation of moral precepts with their former convictions about the existence and binding character of fundamental rights is beyond the scope of this Article. One might speculate, however, that the sheer ubiquity and vehemence of the rhetoric of fundamental rights may help to obscure the absence of a sound moral foundation for that rhetoric from of those who use it.

[287] For Weber, "[a] 'ruling organization' will be called 'political' insofar as its existence and order is continuously safeguarded within a given *territorial* area by the threat and application of physical force on the part of the administrative staff." WEBER, *supra* note 246, at 54 (emphasis in original).

[288] *See supra* note 27 and accompanying text.

apparently do not pose a Hobbesian threat to myself or others, perhaps because I am not viewed simply as an individual pursuing arbitrary personal preferences.[289] My needs and actions therefore cannot be cited to justify expanding the power of bureaucracy. Again, it appears that a different paradigm may be needed to account for our situation within the purely personal space demarcated by the Directive.

As discussed above,[290] one of the key characteristics of the bureaucracy for Weber is the expectation that bureaucrats will deal with official business in an expert and depersonalized manner. This means that a DPSA official, i.e., a bureaucrat within the DPSA, would be expected to develop expertise on issues related to collection and use of PII and on the application of national laws implementing the DP Directive. The official would be expected to approach his or her official business impersonally, i.e., without regard to his or her own personal characteristics or PII. As Dean Kronman wrote, summarizing Weber, "[i]mpersonal rule . . . means that the bureaucrat's personal affairs—his own interests and feelings—must be excluded, insofar as is humanly possible, from the performance of his official duties . . . ."[291] In addition to disregarding his or her own PII, the official would be expected to examine the PII of regulated parties impersonally as a commodity subject to regulatory control and thus ensure that the PII itself—e.g., an individual's wealth or race or nationality—has no impact on the outcome of regulatory action.

The bureaucrat's ability to act as an impersonal expert is one of the primary justifications typically offered under the post-Enlightenment paradigm for granting to public bureaucracies the vital role of imposing order on a world of individuals pursuing personal preferences. In MacIntyre's words, "the major justification advanced for the intervention of government in society is the contention that government has resources of competence which most citizens do not possess."[292] He adds: "Civil servants . . . justify themselves and their claims to authority, power and money by invoking their own competence as scientific managers of social change."[293] Developing MacIntyre's point, I would argue that the impersonal expertise of the bureaucrat provides, or is thought to provide, a guarantee that the bureaucrat will not take sides in the conflicts between the values of the individuals and organizations that the bureaucrat regulates. In place of a shared vision of the good, the impersonal public official offers the promise of a neutral expert charting a path through the terrain of conflicting individual values along a line supposedly dictated by, in Weber's words, "calculable rules and 'without regard for persons.'"[294] In the field of privacy protection, the DPSA official is an impersonal, neutral expert applying calculable rules based on national law implementing the DP

---

[289] *See supra* notes 189–92, 239–242 and accompanying text.

[290] *See supra* notes 245–246 and accompanying text. The claim that bureaucrats are expected to meet certain expectations and thus embody a model of bureaucratic conduct does not mean that any actual bureaucrat succeeds in meeting the standards or embodying the model. These comments about impersonal expertise relate to the ideal type of the bureaucrat. For a discussion of "ideal types," *see, e.g.*, GIDDENS, *supra* note 248, at 141–43; Parsons, *supra* note 244, at 12–13.

[291] ANTHONY T. KRONMAN, MAX WEBER 65 (1983), *quoting* Max Weber, *supra* note 246, at 225.

[292] MACINTYRE, AFTER VIRTUE, *supra* note 12, at 85.

[293] *Id.* at 86.

[294] *See supra* note 246 and accompanying text.

Directive. Standing outside of and above the world of conflicting individual values, including privacy preferences, the DPSA official exercises power over individuals and organizations to prevent chaos and ensure that the outcomes of trading in the PII market are acceptable.

The importance of impersonality in this account of the bureaucrat points to a paradox in the rationale for administrative protection of personal privacy and PII under the post-Enlightenment paradigm. By invoking the fundamental right to privacy, the DP Directive signals the great significance to the individual of PII and its protection, whether a particular individual appreciates that significance or not. Presumably one reason why my PII is significant is that it tells me and others who I am and it distinguishes me from all other individuals as this particular individual. In this sense, it is a substantial component of my personal identity.[295] In order to protect my PII and the related personal identity, however, the post-Enlightenment paradigm presumes and requires intervention and control by a radically impersonal character or persona, the expert DPSA official. Thus, paradoxically, the existence and activity of the impersonal bureaucrat is understood to be a necessary condition of the protection and preservation of PII and personal identity. In other words, under the post-Enlightenment paradigm, protecting the individual's personal identity in the market from threats by other individuals and organizations presupposes cancelling or bracketing out the public official's personal identity. My personal identity can be secure only under the supervision of someone who, qua public official, eschews his or her personal identity and ignores mine.

The paradoxical relationship of impersonal bureaucrat to personal identity points to another paradox in the DP Directive's treatment of the impersonal bureaucrat himself or herself. If the demand for privacy protection is understood as a demand for, among other things, greater bureaucratic authority over collection and use of PII, then it follows that growing concerns about privacy are likely to be met under the post-Enlightenment paradigm with expanding government power. By purporting to regulate government collection and use of PII,[296] however, the DP Directive itself acknowledges that government bureaucracies pose a significant threat to personal privacy. This suggests that each increase in the power of DPSA officials to protect privacy also may enhance the power of those officials to invade privacy. Indeed, the Directive formalizes this power to threaten privacy by explicitly granting DPSA officials seemingly unlimited authority to scrutinize PII.[297] The Directive apparently acknowledges the seriousness of the threat to privacy that it creates and seeks to neutralize the threat by placing DPSA officials under the seal of confidentiality.[298] Thus, the DPSA official embodies a paradox: unlimited power to invade individual privacy that is at the same time sufficient protection of individual privacy. Without this equation of privacy invasion and privacy protection, the DPSA official could not function as the impersonal expert bureaucrat whose activity is necessary to protect the individual's PII and personal identity.

---

[295] *See supra* p. 43–45.
[296] *See supra* note 44 and accompanying text.
[297] *See supra* note 61 and accompanying text.
[298] *See supra* note 62 and accompanying text.

Underlining the paradoxical nature of the DPSA official, it should be recalled that the DP Directive recognizes another sphere in which unlimited power to invade privacy apparently is at the same time sufficient protection of privacy.[299] PII held in the purely personal space is not subject to the Directive or, apparently, the fundamental right to information privacy. Within the purely personal space, a person such as a wife or boyfriend may collect and use PII about another person and yet apparently not pose any threat to the other's privacy. This means that a DPSA official who scrutinizes PII but does not threaten privacy is expected to respect everyone's PII in a way that is eerily similar to the way in which my hypothetical boyfriend is expected to respect my PII. Of course, the hypothetical boyfriend is not under a legal obligation to keep my PII confidential. But the need to impose such an obligation on the DPSA official reveals the extraordinary level of power and trust that the Directive reposes in the DPSA official, power and trust required to receive unlimited access to PII. As indicated above,[300] it is difficult to account for this kind of trust in the purely personal space using the analytical tools of the post-Enlightenment paradigm—i.e., individuals pursuing private preferences according to personal values in a market overseen by impersonal bureaucrats. To account for the character of the boyfriend or the bureaucrat in a manner that justifies reposing trust in either may require reference to a different paradigm.[301] Again, I will simply suggest that the old Aristotelian paradigm, with its emphasis on the virtues and characters of persons in relationships with one another, might provide a useful starting point.

V. THE PRIVACY DEBATE AS FAMILY FEUD

This Article began with the observation that critics of the U.S. internet privacy regime often point to the EU regime as a possible model for law reform in the United States. It is not surprising that scholars might take this position,[302] since an international orientation coupled with an attack on U.S. legal arrangements may lead to publication and academic success. Indeed, criticism of the U.S. regime in light of the EU model has now become sufficiently commonplace that one finds it in law school casebooks. For example, Professors Mann and Winn observe that the OECD's *Guidelines on the Protection of Privacy and Transborder Flows of*

---

[299] *See supra* notes 182–192 and accompanying text (discussing the implications of the DP Directive's exclusion of the purely personal space).

[300] *See supra* pp. 36-37.

[301] *See supra* p. 37.

[302] *See, e.g.*, Jennifer M. Myers, Note, *Creating Data Protection Legislation in the United States: An Examination of Current Legislation in the European Union, Spain, and the United States*, 29 CASE W. RES. J. INT'L L. 109, 113 (1997) (United States should adopt legislation conforming to EU law); Rachel K. Zimmerman, Note, *The Way the "Cookies" Crumble: Internet Privacy and Data Protection in the Twenty-First Century*, 4 N.Y.U. J. LEGIS. & PUB. POL'Y 439, 460, 462–63 (2000–0001) (United States should adopt EU data protection principles and seek EU help in formulating new legislation). *See also* Graham Pearce & Nicholas Platten, *Orchestrating Transatlantic Approaches to Personal Data Protection: A European Perspective*, 22 FORDHAM INT'L L. J. 2024, 2049 (1999) ("fragmentation of U.S. data protection responsibilities is likely to become increasingly apparent as the EU directive becomes operational and appropriate institutional arrangements in the United States would seem essential, both to defend its business interests and to resolve potential political friction between the Union and the United States").

Personal Data "serve as a source of inspiration for the EU data-protection law," while "the United States has not forced its businesses to comply with the *Guidelines*."[303] In a similar vein, Professors Ku and Lipton have written that "[i]n contrast [to the United States], other nations, and most notably, the European Union have taken more aggressive steps to protect individual privacy in data collection."[304] In addition to such scholarly criticism of the U.S. regime from an EU perspective, policymakers and others have strongly suggested that the U.S. regime is not "adequate"[305] from the standpoint of the EU rules restricting exports of PII and should therefore be reformed to facilitate such exports.[306]

For purposes of this Article, the details of the debates about the relative merits of the U.S. and EU regimes are not particularly important. What matters is that by positing the regimes as alternatives, emphasizing the differences between them, and attacking one from the perspective of the other, these debates tend to obscure what the two regimes have in common. As this Article and its predecessor on the U.S. regime have argued, both regimes reflect and reinforce the post-Enlightenment paradigm. Both regimes presume a world consisting of individuals trading their PII in a market as a commodity for a price and both regimes reinforce that world by purporting to protect those individuals and ensure the proper operation of that market. Both regimes presume that individuals will interact with private bureaucratic organizations in the market. Both regimes facilitate and encourage such interactions by subjecting them to regulatory oversight. Both regimes presuppose that the market will not function properly without some degree of public bureaucratic supervision—relatively limited policing supervision under the U.S. regime and relatively more comprehensive market-corrective supervision under the EU regime. Both regimes respond to this presumed need for bureaucratic supervision by purporting to provide the type of supervision supposedly required. In all of these respects, debate over the relative merits of the U.S. and EU information privacy regimes is a family feud because both regimes unmistakably reflect and reinforce the post-Enlightenment paradigm.

Regardless of differences in detail, arguments favoring the U.S. or the EU approach to information privacy on the internet reflect and reinforce the post-Enlightenment paradigm in another important way. As MacIntyre has suggested, in the culture of bureaucratic individualism, political debate typically centers around the merits of extending bureaucratic control.[307]

> [T]he contending parties agree . . . that there are only two alternative modes of social life open to us, one in which the free and arbitrary choices of individuals are sovereign and one in which the bureaucracy is

---

[303] MANN & WINN, *supra* note 3, at 209.

[304] RAYMOND S. R. KU & JACQUELINE D. LIPTON, CYBERSPACE LAW 544 (2d ed. 2006)

[305] *See supra* note 118 and accompanying text; Kightlinger, *supra* note 49, at 10–08.

[306] MANN & WINN, *supra* note 3, at 215. *See* Mike Ewing, Comment, *The Perfect Storm: The Safe Harbor and the Directive on Data Protection*, 24 HOUS. J. INT'L L. 315, 336 (2002) (EU pressured United States to adopt the "Directive or its own comprehensive data protection scheme"); Gregory Schaffer, *Globalization and Social Protection: The Impact of EU and International Rules in the Ratcheting Up of U.S. Privacy Standards*, 25 YALE J. INTL L. 1, 6 (2000) ("EU policy and practice places pressure on U.S. regulators and businesses to adapt U.S. data privacy policy and practice").

[307] *See supra* notes 31–32 and accompanying text.

> sovereign, precisely so that it may limit the free and arbitrary choices of individuals.[308]

To illustrate MacIntyre's point, I have shown elsewhere that a recent political debate in the United States about the freedom of children to use the internet without risks to information privacy resulted in, among other things, an extension of the FTC's authority over children's PII.[309] What began as a debate about protecting individual freedom ended by, among other things, enhancing bureaucratic control. Similarly, any debate over the relative merits of the U.S. and EU approaches to information privacy inevitably will oscillate between these same poles, favoring some version of the U.S. approach, which emphasizes the sovereignty of the free individual in the market, or some version of the EU approach, which emphasizes bureaucratic control over the market, or some hybrid of the two approaches.[310] Thus, what initially seemed like a novel debate about information privacy in the new electronic media simply reprises a long-standing debate or antinomy—individual v. bureaucracy—rooted in the collapse of the old teleological paradigm and the rise of bureaucratic individualism under the new post-Enlightenment paradigm.

Alfred North Whitehead once wrote, presumably with some irony, that "[f]amiliar things happen, and mankind does not bother about them. It takes a very unusual mind to undertake the analysis of the obvious."[311] Whitehead's comment seems particularly apposite to comparisons between the U.S. and EU internet privacy regimes. There is something strangely obvious and familiar about the elements that the two regimes have in common, i.e., individuals, markets, bureaucracies, and there is something obvious and familiar about a debate pitting the more individualist U.S. approach against the more bureaucratic or "statist" EU approach. The role of the post-Enlightenment paradigm as a conceptual foundation for both regimes and for the debate between them helps to explain the pervasive sense of obviousness and familiarity. If, as has been argued in this Article and its predecessor, the post-Enlightenment paradigm guides and structures the way that we ordinarily think about ourselves and our institutional world, then we would find it obvious and familiar that the U.S. and EU regimes take the forms that they do and that debates about online privacy oscillate between these two poles. Indeed, we would find it very difficult to imagine the regimes looking otherwise or the debate taking any other form. This simply *is* the way our political life now looks and, as MacIntyre suggests, this *is* the way debate about political issues unfolds. In this respect, the foundational presence of the post-Enlightenment paradigm may help to explain the obviousness of the obvious and the familiarity of the familiar. And this strong feeling of obviousness and familiarity lends support to the contention that the post-Enlightenment paradigm is *our* paradigm.

No doubt proponents of one or the other internet privacy regime would find this discussion simplistic and misleading because it deflects attention from what they

---

[308] MACINTYRE, AFTER VIRTUE, *supra* note 12, at 35.

[309] Kightlinger, *supra* note 7, at 389 (discussing Congress's adoption of COPPA).

[310] For an interesting example of a hybrid approach, see Schwartz, *supra* note 2, at 1679–81 (calling for, among other things, establishment of a U.S. Data Protection Commission modeled after the national data protection agency in Canada or the DPSA in Germany).

[311] ALFRED N. WHITEHEAD, SCIENCE AND THE MODERN WORLD 4 (1953).

would say is the real and important issue. They would point out that despite the structural similarities between the two regimes, there are real differences, and those differences present us with a policy choice: which regime should we adopt and why? Our real and important task is to reason and debate our way to the correct choice, and not to spin our wheels discussing paradigms. The difficulty with this way of characterizing our situation—i.e., as people who must engage in a process of reasoned policy choice—is that it invites a further swing of the post-Enlightenment hammer. If the Enlightenment critique of earlier teleological schemes was correct, then we no longer have available to us a true account of the human good or *telos*. If the subsequent critique of Enlightenment thought is correct, then we also do not have available to us an adequate substitute for the earlier teleological schemes, a substitute that provides adequate reasons for embracing the list(s) of moral and ethical precepts by which each of us ordinarily lives. Under the post-Enlightenment paradigm, those precepts are now understood to reflect our private, subjective values, and not a true account of who we are and who we should become. The precepts are understood to display, in MacIntyre's phrase, arbitrary preferences. Thus, in attempting to perform the "real and important task" of reasoned policy choice, one may be able to demonstrate that commitment to a particular internet privacy regime, to an individualist approach or a bureaucratic approach, is consistent with, and perhaps follows logically from, a particular set of moral and ethical precepts. But under the post-Enlightenment paradigm, this demonstration also appears to prove that commitment to a particular approach to internet privacy is ultimately rooted in an individual's private values and arbitrary preferences.

If a reasoned policy choice between competing approaches to internet privacy will reflect nothing more than the arbitrary preferences of the person doing the choosing, then at bottom, the choice will be arbitrary. My choice will, of course, not seem arbitrary to me, because it will reflect my preferences, and my preferences do not seem arbitrary to me. My preferences catalogue what matters to me, and surely what matters to me cannot be arbitrary. But this attempt to explain and justify my policy choice by reference to my preferences begs the question why my preferences matter, or should matter, to me or anyone else. Under the post-Enlightenment paradigm, my preferences appear to be a fact about me from which no value, no "ought" statement, can be inferred.[312] So a process of reasoned policy choice may show me the logical implications of what are in fact my preferences in the field of information privacy, but that process cannot show me or anyone what I ought to prefer and why. Under the post-Enlightenment paradigm, my preferences and values simply are what they are. Thus, focusing on the foundational role of the post-Enlightenment paradigm in the EU and U.S. internet privacy regimes does not simply deflect us from the real and important task of reasoned policy choice. It actually may encourage us to depose, or at least challenge, such idols of Enlightenment faith as the very possibility of reasoned policy choices. We may have to recognize that reasoned policy choice is another moral fiction masking arbitrary preferences. This line of argument clearly raises a host of serious questions discussion of which must be deferred to a later publication. One thing should, however, be clear. We cannot simply presume that making a policy choice between

[312] *See supra* notes 22–23 and accompanying text.

the two competing approaches to internet privacy is our real and important task. Indeed, we cannot presume that we are even capable of answering the moral/ethical question which of our tasks is or are real and important, because this question will pose a central problem in any discussion of the post-Enlightenment paradigm and its implications.

This argument regarding the foundational role of the post-Enlightenment paradigm is not intended to imply that there will in fact be no resolution to the debate over the relative merits of the EU and U.S. internet privacy regimes. Rather, it is intended to suggest that under the paradigm any proposed resolution will reflect only the arbitrary preferences of those who favor that resolution and will make no claim, reasoned or otherwise, on those who do not share such preferences. Any "victory" for one or the other proposed resolution will reflect only the arbitrary balance of forces supporting competing arbitrary personal preferences. To pursue the analogy suggested above, if the debate over the relative merits of the U.S. and EU approaches to information-privacy protection is a kind of family feud, then the family itself is fundamentally dysfunctional because the feud cannot be definitively settled under the post-Enlightenment paradigm without resort to force. The feud is interminable, and it will demonstrate its interminability by reappearing time and again. Any "resolution" to the feud will last only as long as the victors remain in the ascendancy.

The EU's export-control regime for PII nicely illustrates the role of political and economic force in the "debate" over competing approaches to protecting PII. The DP Directive tightly restricts exports of PII to countries that lack "adequate" privacy protection[313] and requires the European Commission to "enter into negotiations" with such countries "with a view to remedying the situation."[314] In effect, the Directive threatens to "embargo" PII exports to countries that refuse to play ball,[315] thereby forcing such countries to revise their national laws and then ask DPSA and EU officials to bless the result. Thus, as one would expect under the post-Enlightenment paradigm, European bureaucrats may settle the "debate" in most countries over the merits of competing approaches to information privacy by wielding thinly disguised economic force in favor of the more bureaucratic EU approach.[316] That we continue to refer to this international process as a "negotiation" and the ensuing domestic political affray as a "debate" demonstrates again our susceptibility to moral fictions.

---

[313] *See supra* Part III.B.3.

[314] *See* DP Directive, *supra* note 42, art. 25.5.

[315] *See id.* art. 25.4. I owe the term "embargo" to Paul Schwartz. *See* Schwartz, *supra* note 42, at 488–95 (discussing the possibility that data protection officials might embargo data exports to countries lacking adequate protection).

[316] The EU-U.S. Safe Harbor Agreement, *see supra* note 116, illustrates what can happen in negotiations over PII exports and national law reform when an irresistible bureaucratic force from the EU meets an immoveable bureaucratic object such as the U.S. Department of Commerce backed by U.S. industry. The resolution of the "debate" reflects the balance of forces.

VI. CONCLUSION

This Article began with an outline of the origins of what I have labeled the "post-Enlightenment paradigm," a notion that I derived from the philosophical work of Alasdair MacIntyre. The Article then discussed the EU's information-privacy regime in some detail and sought to show that the regime reflects and reinforces the post-Enlightenment paradigm. The regime reflects the paradigm because the regime is constructed around the paradigm's key elements: individuals, markets, and bureaucracies. It reinforces the paradigm because it provides legal support for those elements. The regime abstracts people from "purely personal" relationships and deals with them as individuals; it treats interactions between and among individuals and organizations as market interactions in which each party exchanges items of value, including PII, for a price; and it imposes bureaucratic supervision on individuals, organizations, and their interactions. Moreover, the information-privacy regime reflects and reinforces the paradigm in a field of supposedly intimate significance to people and their personal identities, i.e., collection and use of PII. Indeed, it is one of the paradoxes of a world organized around the post-Enlightenment paradigm that the "obvious" response to concerns about threats to our intimate, personal lives is expanding the power of an impersonal, expert bureaucracy—in this instance the DPSAs in the EU Member States.

Drawing on my conclusions in a previous study, this Article also has sought to show that the U.S. and EU internet privacy regimes have a common structure rooted in the post-Enlightenment paradigm. This strongly suggests that debates about the relative merits of the two regimes, regardless of differences in detail, will also strengthen the hold of the paradigm. Under the paradigm, we find ourselves living in the culture of bureaucratic individualism, and debates about public policy issues predictably become debates about which side of the dyad, individual or bureaucracy, to emphasize at any given time. The U.S. internet privacy regime emphasizes the former, the EU regime the latter, and together they appear to define our principal options. If, as I have suggested, the post-Enlightenment paradigm is our normal and ordinary way of explaining and justifying human action, then it is not surprising that the options presented by the paradigm—individual or bureaucracy—might appear to be the primary, if not the only options available to us. Indeed, it would not be surprising if these options and the debate they engender would come to seem obvious and familiar, precisely because the paradigm limits our ability to imagine and articulate plausible alternatives.

This Article's conclusions concerning the role of the post-Enlightenment paradigm in shaping and structuring our thinking should be regarded as provisional. It is one thing to find operating in the U.S. and EU internet-privacy regimes certain philosophical presumptions that emerged from the wreckage of Enlightenment thought and quite another to conclude that those presumptions constitute a paradigm that shapes and structures the way that we think. In a projected study of early U.S. Supreme Court decisions examining and defining the authority of the Interstate Commerce Commission, I expect to provide further evidence of the role that the post-Enlightenment paradigm plays in shaping reflection on policy issues. A working hypothesis of that study will be that one can identify in the Court's

reasoning clear evidence of the paradigm's emergence as a distinctive explanation and justification of human action in the rapidly industrializing Nineteenth Century United States. A broader methodological goal of the projected study will be to demonstrate that the post-Enlightenment paradigm provides a useful heuristic device for reassessing the significance of seemingly familiar legal developments and institutions far afield from information privacy, and relating those legal developments and institutions to broader historical and philosophical trends discussed in MacIntyre's work.

Assuming it is possible to demonstrate through a series of studies the pervasive impact of the post-Enlightenment paradigm on the way that we explain and justify human action in the fields of law and administration, there nevertheless will remain an arguably more basic question: is there an alternative to the post-Enlightenment paradigm? Identifying a paradigm and tracing its influence is not the same as escaping or transcending a paradigm.[317] As noted above,[318] to escape from the post-Enlightenment paradigm, one presumably would have to pursue one of two approaches. One approach would be to assist in the revival of the pre-Enlightenment teleological account of human nature and moral life, building on the moral and political philosophy of Aristotle. By way of illustration, this Article has noted at several points problems or questions that arise under the DP Directive and the post-Enlightenment paradigm that the old Aristotelian paradigm might help us to address and perhaps resolve.[319] Revitalizing the old paradigm has been a key thrust of MacIntyre's work over the last twenty years.[320] In future articles, I expect to examine and pursue MacIntyre's endeavors in this direction, focusing on his discussions of natural law and questioning the usefulness of his effort to defend a Christian and Thomist interpretation of Aristotle.[321]

Instead of attempting to breathe life into a moldering Aristotle, an alternative approach would be to accept as decisive the Enlightenment's critique of the older teleological framework and attempt to construct a new rational basis or intellectual support structure for our moral/ethical and political/legal commitments. Latter-day Kantians, utilitarians, and others might be viewed as engaging in this task. For reasons summarized by MacIntyre, however, I am much less sanguine about this approach:

> [T]he great Enlightenment theorists had themselves disagreed both morally and philosophically. Their heirs have, through brilliant and sophisticated feats of argumentation, made it evident that if these disagreements are not interminable, they are such at least that after two hundred years no prospect of termination is in sight. Succeeding

---

[317] Kightlinger, *supra* note 7, at 354–55.

[318] *See supra* note 211.

[319] *See supra* pp. 35–36 and note 242 and accompanying text. *See also supra* pp. 61-62.

[320] For a brief and accessible defense of Aristotelian moral theory, see ALASDAIR MACINTYRE, *Plain Persons and Moral Philosophy: Rules, Virtues and Goods*, *in* THE MACINTYRE READER 136 (Kelvin Knight ed., 1998).

[321] MACINTYRE, THREE RIVAL VERSIONS, *supra* note 12, at 170–215 (arguing that the Aristotelian-Thomist emphasis on traditions of moral enquiry may help to identify and possibly resolve problems in competing moral frameworks).

> generations of Kantians, utilitarians, natural rights' theorists, and contractarians show no sign of genuine convergence.[322]

I would be pleased to see progress toward such a convergence or a persuasive explanation of why convergence is not possible or desirable. As matters stand, however, perpetual disagreement among the main modern schools of moral philosophy tends to bolster the post-Enlightenment paradigm by lending credibility to the thesis that our conflicting moral beliefs necessarily reflect nothing more than the private, ultimately arbitrary preferences or values of the particular believer—even if that believer bears the title Professor of Philosophy and can fashion his or her beliefs into a book-length argument. My working hypothesis would be that Aristotle can provide a way out of the impasse of Enlightenment and post-Enlightenment moral philosophy and that his work therefore may still provide the basis for a persuasive alternative to the post-Enlightenment paradigm.

[322] ALASDAIR MACINTYRE, *Some Enlightenment Projects Reconsidered*, *in* ETHICS AND POLITICS 172, 181–82 (2006). MacIntyre has argued persuasively that there is still a great deal to be learned from utilitarian and Kantian approaches to moral philosophy, even if those approaches ultimately leave fundamental questions unanswered. *See* ALASDAIR MACINTYRE, *Truthfulness and Lies: What is the Problem and What Can We Learn from Mill?*, *in* ETHICS AND POLITICS 101–21 (2006) (drawing insights from Mill's utilitarianism); ALASDAIR MACINTYRE, *Truthfulness and Lies: What Can We Learn from Kant?*, *in* ETHICS AND POLITICS 122–42 (2006) (drawing insights from Kant's moral philosophy).