Harvard Journal of Law & Technology
Volume 18, Number 1 Fall 2004

PRIVACY IN ATLANTIS*

*Jerry Kang & Benedikt Buchner***

TABLE OF CONTENTS

---

* This paper was funded in part by UCLA School of Law, Harvard Law School, and UCLA Asian American Studies Center. This paper has been presented at the Berkman Center cyberlaw retreat and the Washington DC Privacy Law scholars group. The Hugh & Hazel Darling Law Library at UCLA School of Law provided expert research assistance. For helpful comments and suggestions on previous drafts, the authors thank Julie Cohen, Lance Hoffman, Justin Hughes, Hassan El Menyawi, William Fisher, Robert Gellman, Do Kim, Sung Hui Kim, Gerda Kleijkamp, Charles Nesson, Manuel Nodoushani, Chris Noofnagle, Jeffrey Rosen, Marc Rotenberg, Paul Schwartz, Joseph Singer, Daniel Solove, Sonia Suter, Peter Swire, Tsubasa Wakabayashi, Rolf Weber, Jonathan Weinberg, and Jonathan Zittrain.

** Jerry Kang is Visiting Professor of Law, Georgetown Law Center; Professor of Law, UCLA School of Law. Email: kang@law.ucla.edu; website: http://jerrykang.net. Benedikt Buchner is Lecturer, University of Munich, Institute for International Law. Email: b.buchner@jura.uni-muenchen.de.

INTRODUCTION

The nation state of Atlantis is a modern society in all respects, including culture, economics, and technology. But it is still ruled by a benevolent monarch, the Queen, who has successfully forged consensus through wise deliberation and the advice of her faithful and pragmatic Counselor.[1] *The rise of cyberspace has prompted numerous questions about law and policy within Atlantis. Privacy stands prominently among these concerns. The Queen has just charged the Counselor to consult learned stakeholders to forge a course of action. The Queen expects prompt and practical answers, so the Counselor must respond quickly. He has called forth the Philosopher, Economist, Merchant, and Technologist. The scene starts in the great Hall of Discussion.*[2]

[Counselor pushes open the great doors to the Hall of Discussion to hear a pitched conversation between Philosopher and Economist, standing respectively to Counselor's left and right, across a long, ornately carved wooden table. Technologist and Merchant are seated farther down the table, across from each other.]

Philosopher [to Economist]: But you demean human dignity to speak in such terms. The sanctity of personality is inconsistent with selling privacy in the marketplace, for baubles.

---

1. Our title might recall Francis Bacon's *New Atlantis*, published in 1624. In Bacon's unfinished utopian dream, he envisioned a technologically advanced society "based on a system of secrets," which "a modern liberal" would find "oppressive . . . hierarchical, [and] intolerant." DANIEL R. COQUILLETTE, FRANCIS BACON 261 (1992). We do not intend to create here any parallel to Bacon's utopia; however, we acknowledge that Bacon presciently understood the power and the double-edged nature of scientific technology, and that the power of technology "would require social and political discipline of a new order." *Id*. at 262. Bacon's title itself harks back to Plato's unfinished account of Atlantis in his *Timaeus* and *Critias*. *See id*. at 261.

2. The characters in the dialogue are fictional caricatures, constructed to drive a pedagogically telling conversation. The caricatures are not, however, so grotesque as to miscapture philosophical and policy positions seriously held by real stakeholders in the privacy debate. Of course, first-rate academic inquiry from, for example, a real philosopher or economist would provide more careful and comprehensive arguments than those presented in the dialogue. But providing such details and qualifications would produce a boring read, which would be entirely inconsistent with the unusual form and purpose of this project. Those serious arguments can be found in the work of scholars cited throughout the footnotes. Authors' commentary about the dialogue appears in the Appendix.

Economist [back at Philosopher]: You use quaint terms such as "dignity" that I do not know how to operationalize.[3] If people prefer dignity, they will acquire it in the marketplace, like they acquire most everything else. And if they choose not to, that is evidence that they did not want it in the first place — notwithstanding what academic elites have to say.

Counselor [interrupting]: Ahem. I see that the conversation has already started. [Everyone bows politely to Counselor.] As you all know, the Queen has charged me with advising her on privacy issues in our great nation of Atlantis. Time is of the essence, and I confess that I know far less about the matter than I should. This much I do know: new information technologies, especially digital ones, threaten privacy gravely,[4] and the citizenry is concerned. But *what* we should do about it, if anything, is unclear. Let us talk seriously about how we might properly think about the problem.[5] Who shall begin the discussion?

SCENE I: PRIVACY'S FORM

A. Market-Talk

Economist: If I may, dear Counselor, as you know, privacy concerns the flow of personal data — information about ourselves. That flow of information is critical to a well-functioning economy and society. If there is some conflict about how personal data should be used, I suggest that we resolve that conflict the same way we allocate any other resource in Atlantis — through the free market. Why reinvent the wheel? Simply consider personal data to be a "widget," and let the market decide who ends up controlling it.

---

3. *Cf.* Julie E. Cohen, *DRM and Privacy*, 18 BERKELEY TECH. L.J. 575, 607 (2003) (noting that in current academic and policy circles, "arguments from human dignity seem both insufficiently rigorous and vaguely passe").

4. For a comprehensive overview of the current problems and potential risks for data privacy, see, for example, A. Michael Froomkin, *The Death of Privacy?*, 52 STAN. L. REV. 1461, 1468–1501 (2000); Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193, 1220–41 (1998); Daniel J. Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy*, 53 STAN. L. REV. 1393, 1400–13 (2001). Some commentators have already announced the "end," "death," and "destruction" of data privacy in America's twenty-first century. *See, e.g.*, SIMSON GARFINKEL, DATABASE NATION: THE DEATH OF PRIVACY IN THE 21ST CENTURY (2000); JEFFREY ROSEN, THE UNWANTED GAZE: THE DESTRUCTION OF PRIVACY IN AMERICA (2000); REG WHITAKER, THE END OF PRIVACY (1999).

5. American legal scholars have proposed a wide variety of approaches to address information privacy. For a survey of the different approaches to data privacy, see ROLF H. WEBER, REGULATORY MODELS FOR THE ONLINE WORLD 160–70 (2002).

Merchant [interjecting]: I could not agree more with the brilliant Economist. The free market is sufficient. And recall that the free market has kept Atlantis flourishing in growth and trade.

Counselor: Interesting. Economist, do you mean to say that we should consider personal data to be no different than physical *property*, like this pen? [Counselor waves pen in the air.]

Economist: Dear Counselor, to be careful, I should clarify that a free-market approach could be implemented in various ways. For example, a full *property* approach would, as you suggest, treat personal data as intangible property whose allocation and exchange is determined by free-market interactions.[6] Closely connected, but not identical, the *contract* approach puts party agreement[7] at the heart of personal data processing. Regardless of whether personal data are viewed entirely as property, the contractual approach allows parties to make promises regarding personal data and the processing of data.

Counselor: What exactly is the difference between the *property* and the *contract* approaches? After all, doesn't viewing something as property mean that it can be traded, through contract?[8]

---

6. Many commentators have recommended a property approach solution. *See Developments in the Law — The Law of Cyberspace*, 112 HARV. L. REV. 1574, 1644–48 (1999) (preferring a property rule to a liability rule for the protection of privacy in cyberspace); Edward J. Janger, *Privacy Property, Information Costs, and the Anticommons*, 54 HASTINGS L.J. 899 (2003) (arguing for a switch to property-based protection of personal data); Kenneth C. Laudon, *Markets and Privacy*, Comm. ACM, Sept. 1996, *at* 92 (suggesting a regulated "national information market" where personal information can be bought and sold); LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE 159–62 (1999) (arguing for property rights in privacy as a pragmatic response to the actual commercial use of personal data); Richard S. Murphy, *Property Rights in Personal Information: An Economic Defense of Privacy*, 84 GEO. L.J. 2381, 2383–84 (1996) (stating that "[personal] information, like all information, is property"); James Rule & Lawrence Hunter, *Towards a Property Right in Personal Data*, *in* VISIONS OF PRIVACY: POLICY CHOICES FOR THE DIGITAL AGE 168 (Colin J. Bennett & Rebecca Grant eds., 1999) (proposing the creation of a property right over commercial exploitation of personal information); Carl Shapiro & Hal R. Varian, *US Government Information Policy* (1997), *at* http://www.sims.berkeley.edu/~hal/Papers/policy/policy.html (suggesting assignment of property rights in information to individuals and allowing them to contract with other parties about how they might use the information); Hal R. Varian, *Economic Aspects of Personal Privacy*, *in* PRIVACY AND SELF-REGULATION IN THE INFORMATION AGE ch. 1, C (U.S. Dep't of Commerce ed., 1997), *available at* http://www.ntia.doc.gov/reports/privacy/privacy_rpt.htm [hereinafter ECONOMIC ASPECTS]; *see also* RICHARD A. POSNER, ECONOMIC ANALYSIS OF LAW 46 (1998) (viewing data privacy law functionally as "a branch of property law").

7. This agreement may be called a contract or license. *See, e.g.*, Pamela Samuelson, *Privacy As Intellectual Property?*, 52 STAN. L. REV. 1125 (2000) (arguing for a contractual approach in combination with a set of default licensing rules adapted from trade secrets law); Kalinda Basho, Comment, *The Licensing of Our Personal Information: Is It a Solution to Internet Privacy?*, 88 CAL. L. REV. 1507 (2000) (advocating a licensing system for personal information that gives the contracting parties the right to determine the terms of the contract).

8. In many analyses, the property and contractual approaches are entangled and are assumed to be a pair. Even if these approaches are distinguished, readers may not see much of a difference. In one of our papers, for example, there was an attempt to avoid a full property

Economist: Yes, Counselor, you are perceptive to note the overlap. However, some nontrivial differences have made a number of *contract* proponents remain agnostic[9] or hostile to the *property* approach.[10] For instance, if commodification is a concern . . .

Philosopher [interjecting]: And why should it not be?

Economist [continuing]: . . . allowing only contracting about personal data may pose fewer difficulties than full propertization.[11] In addition, creating property rights in personal data risks some inconsistency with our intellectual property laws, which do not grant ownership in facts — personal or otherwise.[12]

Counselor: Hmm . . . I see. But let us not get bogged down in details. Notwithstanding these sometimes important differences, both approaches frame the privacy matter in market terms. I gather, then, that they trumpet similar benefits — allocative efficiency,[13] individual freedom, flexibility, and so on.

Merchant: And let's not forget the value of limited state regulation, dear Counselor. By letting the market decide, we give to the citizens of Atlantis the power to choose "their optimal mix of privacy"[14] without parentalistic intervention from the state.[15] This is fully consistent with the whole point of privacy, which is to grant to the individual control over personal data. And it is consistent with the Queen's desire for our citizens to be rugged, self-reliant individuals who exercise discipline and autonomy. We must avoid regulations that spawn mountains of paperwork, which help no one except lawyers and "compliance" bureaucrats.

[Counselor, nodding his head…]

---

conception of a market solution. *See* Kang, *supra* note 4. Yet, many commentators refer to it as a property approach. *See, e.g.*, Jessica Litman, *Information Privacy/Information Property*, 52 STAN. L. REV. 1283, 1290 (2000) (calling Prof. Kang's "market solution" analysis a "market-property rights model").

9. *See, e.g.*, Kang, *supra* note 4.

10. *See, e.g.*, William McGeveran, Note, *Programmed Privacy Promises: P3P and Web Privacy Law*, 76 N.Y.U. L. REV. 1812 (2001); Samuelson, *supra* note 7, *passim*.

11. *See, e.g.*, Samuelson, *supra* note 7, at 1137–38 (raising concerns about accelerating the sell-out of privacy due to the free alienability of property rights).

12. *See* McGeveran, *supra* note 10, at 1839–40; Samuelson, *supra* note 7, at 1140–41. Of course, this could still be seen as a property allocation, one that leaves the facts in the commons.

13. Whether such benefits are in fact achieved depends on whether the conditions for a perfect marketplace are sufficiently satisfied. Such conditions ideally include rational actors, perfect information, zero transaction costs, perfect competition, and no wealth effects. *See* Kang, *supra* note 4, at 1250 & n.242.

14. Steven A. Bibas, *A Contractual Approach to Data Privacy*, 17 HARV. J.L. & PUB. POL'Y 591, 611 (1994).

15. *Id*. at 609 ("In the hands of bureaucrats or judges, flexibility produces uncertainty for private parties. In the hands of the contracting parties, however, flexibility allows people to control their lives and efficiently tailor the law to meet their needs.").

B. Dignity-Talk

Philosopher: If I may, dear Counselor . . . .

Counselor: Yes, patient you have been. Proceed.

Philosopher: Privacy must not be viewed as a commodity. Instead, it must be viewed as a fundamental human right[16] grounded in the dignity of the person.[17] Privacy has intrinsic value in that moral persons deserve some threshold amount of it, notwithstanding the fact that they live in communities. Privacy also modulates intimacy, which has instrumental value in terms of psychic well-being and the construction and deepening of social relationships.[18] As another philosopher has put it, privacy protects "the individual's interest in becoming, being, and remaining a person."[19]

Counselor: You speak eloquently, but practically, what does that mean?

Philosopher: Well, this dignity conception of privacy is reflected in Atlantis' common law, which protects the right of privacy. Our law draws heavily from the common law of the United States, which forged a right of privacy in the twentieth century on the basis of a remarkable article by Samuel Warren and Louis Brandeis.[20] They focused on the affront to human dignity caused by public disclosure of private facts. They called for a right "to be let alone"[21] in the face of increasing prying, to protect an individual's "inviolate personality."[22]

---

16. Convention for the Protection of Human Rights and Fundamental Freedoms, Nov. 4, 1950, art. 8, para. 1, 213 U.N.T.S. 221, 230 (entered into force Sept. 3, 1953) *reprinted in* PRIVACY LAW SOURCEBOOK 2002: UNITED STATES LAW, INTERNATIONAL LAW AND RECENT DEVELOPMENTS, at 318–23 (Marc Rotenberg ed., 2002) [hereinafter PRIVACY LAW SOURCEBOOK] ("Everyone has the right to respect for his private and family life, his home and his correspondence."). The Convention has been signed by forty-three European states, revealing broad support for a human rights approach to privacy.

Furthermore, many constitutions in Europe explicitly recognize the right of privacy and private communications. These include Belgium (Article 22, 29), Finland (Section 10), Greece (Article 9, 9A, 19), Netherlands (Article 10, 12, 13), Portugal (Article 26, 34, 35), and Spain (Article 18). *See* PRIVACY AND HUMAN RIGHTS 2003, 158, 230, 257, 362, 407, 469, 474 (Electronic Privacy Information Center & Privacy International ed., 2003).

17. For a dignity-based conception of privacy, see Edward J. Bloustein, *Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser*, 39 N.Y.U. L. REV. 962 (1964) (viewing privacy as an interest of the human personality that protects the inviolate personality, the individual's independence, dignity, and integrity). There are other philosophical foundations for respecting individual privacy, expressed more in terms of liberty, autonomy, and/or equality. We are not trying to be substantively comprehensive in the dialogue, as that would require an ensemble cast representing an entire philosophy department.

18. *See* Charles Fried, *Privacy*, 77 YALE L.J. 475 (1968).

19. Jeffrey H. Reiman, *Privacy, Intimacy, and Personhood*, in PHILOSOPHICAL DIMENSIONS OF PRIVACY 300, 314 (Ferdinand David Schoeman ed., 1984).

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

21. *Id*. at 195.

22. *Id*. at 205, 211.

As with the courts of the United States, our wise judges have adopted this personal concept of privacy.[23] For us, the right of privacy is a *personal* right, not a *proprietary* one.[24] "The focus of injury in invasion of privacy cases is upon human dignity and peace of mind."[25]

Counselor: Wait, do you mean that our courts have already developed a right of privacy that addresses the problems foisted upon us by digital technologies? Then our task is done!

Philosopher: Well, not precisely, dear Counselor. Our courts, similar to the state courts in the United States, have not construed privacy in a way that especially focuses on *information* privacy.[26] Although some have advocated for creative and expansive reading of the privacy tort,[27] our courts have been conservative in their response.[28]

Merchant [interjecting]: And for good reason!

Counselor: So, alas, work remains. You speak much of the Americans. But I know, Philosopher, that your heart remains with Europe.

Philosopher: The dignity understanding of privacy has been even more strongly embraced in Europe, producing a regulatory system that protects this basic human right. Nearly a decade ago, the European Union enacted its Data Protection Directive.[29] The Directive

---

23. For forty years after the publication of the Warren & Brandeis article, *see id*., courts disputed whether the right of privacy existed at all. By the 1940s, however, "the tide set in strongly in favor of recognition." William L. Prosser, *Privacy*, 48 CAL. L. REV. 383, 386 (1960). *But see* James Q. Whitman, *The Two Western Cultures of Privacy: Dignity Versus Liberty*, 113 YALE L.J. 1151, 1204 (2004) (describing the reception of the Warren & Brandeis concept of privacy as the "story of the relative failure of Warren and Brandeis").

24. *See* J. THOMAS MCCARTHY, THE RIGHTS OF PUBLICITY AND PRIVACY § 1:18 (2d ed., loose-leaf collection).

25. *Id*. at § 11:27.

26. The traditional tort of invasion of privacy encompasses four different privacy torts: intrusion, public disclosure of private facts, false light, and appropriation. This commonly accepted typology traces back to Prosser, *supra* note 23, and is also adopted in RESTATEMENT (SECOND) OF TORTS §§ 652A–652E (1977).

27. *See, e.g.*, Jonathan P. Graham, *Privacy, Computers, and the Commercial Dissemination of Personal Information*, 65 TEX. L. REV. 1395, 1428 (1987) (discussing the recognition of a new tort that addresses unacceptable commercial dissemination of private facts as a means of protecting individual privacy); Litman, *supra* note 8, *passim* (suggesting a privacy approach based on the tort doctrine of breach of confidence); Cohen, *supra* note 3, at 589–600.

28. *But cf*. Remsburg v. Docusearch, 149 N.H. 148 (2003) (holding that information brokers and private investigators could be liable for negligent selling of personal data, which in this case allowed a stalker to locate and murder his victim).

29. Council Directive 95/46/EC, 1995 O.J. (L 281) 31 (*reprinted in* PRIVACY LAW SOURCEBOOK, *supra* note 16, at 367–94) [hereinafter EU Data Protection Directive]. For a discussion of the Directive, see Paul M. Schwartz, *European Data Protection Law and Restrictions on International Data Flows*, 80 IOWA L. REV. 471 (1995); Spiros Simitis, *From the Market to the Polis: The EU Directive on the Protection of Personal Data*, 80 IOWA L. REV. 445 (1995); PETER P. SWIRE & ROBERT E. LITAN, NONE OF YOUR BUSINESS: WORLD DATA FLOWS, ELECTRONIC COMMERCE, AND THE EUROPEAN PRIVACY DIRECTIVE (1998).

comprises detailed rules concerning all aspects of data processing: the confidentiality and security of processing; the criteria for making data processing legitimate; the information to be given to the data subject; the data subject's right of access to data and the right to object to the processing of data; the establishment of supervisory authorities; and available remedies.[30] Many of our most prominent thinkers have encouraged such a framing and approach to privacy.[31]

Merchant [interjecting]: Yes, a true regulatory maze, representing parentalism, rigidness, and top-down regulation. In Atlantis, the Queen has always favored individual freedom, flexibility, and self-regulation,[32] not ex-ante remedies for every possible problem. It is the way of Atlantis. It is what makes us free.

Counselor: Thank you for the reminder, Merchant. But the Queen will decide for herself what she favors. Anyway, freedom is such a complicated matter, isn't it? [Smiles.]

SCENE II: PRIVACY'S SUBSTANCE

Counselor: Now I have a better idea of the controversy. I see Economist's *market* approach on the one hand and Philosopher's *dignity* approach on the other. And I now understand why the discussion has become so embattled, why the rhetoric so fierce. But still I remain confused.

---

30. The EU Data Protection Directive was adopted on October 24, 1995. Its objective is to harmonize European data protection legislation in order to remove potential obstacles to the cross-frontier flows of personal data and to ensure a high level of data protection within the EU. Although the Directive is not directly applicable, it constitutes the cornerstone of European privacy legislation since all Member States must implement the Directive into their national laws.

Member States were to implement The Directive by October 25, 1998, but few Member States met the deadline. Most Member States notified the Commission of their implementation in the years 2000 and 2001. To view the current status of implementation, see Status of Implementation of Directive 95/46 on the Protection of Individuals with regard to the Processing of Personal Data, *at* http://europa.eu.int/comm/internal_market/privacy/law/-implementation_en.htm (last visited Dec. 4, 2004).

31. Proponents of a regulatory approach include Anita L. Allen, *Coercing Privacy*, 40 WM. & MARY L. REV. 723, 755–57 (1999) (arguing for government intervention in order to prevent an erosion of privacy tastes and privacy expectations); Marc Rotenberg, *Fair Information Practices and the Architecture of Privacy: (What Larry Doesn't Get)*, 2001 STAN. TECH. L. REV. 1 (2001) (rejecting Larry Lessig's property model); Paul M. Schwartz, *Internet Privacy and the State*, 32 CONN. L. REV. 815, 858 (2000) (emphasizing the "State's important role in shaping both a privacy market and privacy norms for information in cyberspace").

32. *See* Schwartz, *supra* note 31, at 843–46 (calling these three pairs the dominant rhetoric of cyber-talk: industry self-regulation, bottom-up, and market-based).

A. The Core Similarities

1. Dignity's Consent (or the Market's Initial Allocation)

Counselor: Philosopher, please continue describing the EU's dignity approach.

Philosopher: Thank you, Counselor. The principle of the Directive may be characterized as a prohibition on personal data processing, unless permission is found through certain established means.[33] I apologize for the details, but they are helpful. According to Article 7 of the Directive, personal data may be processed only if either the data subject has given his consent unambiguously[34] or the processing is covered by a statutory exception. Those statutory exceptions are: processing necessary to perform a contract, to comply with a legal obligation, to protect the vital interests of the data subject, to perform a task carried out in the public interest or as an exercise of official authority, or to serve the overriding interest of the controller or a third party . . . .[35]

Merchant [interjecting]: You see, dear Counselor, this is exactly the rigid and parentalistic system of prohibition and detailed regulation I spoke of . . . .

Philosopher [retorting]: I do not regard it so if the Directive leaves it to the individual to decide how her personal data will be processed!

Merchant: But market competition will take care of things. Where is the evidence that the free market approach is failing? The burden must always be on the regulators. Why do you leftist academics naively assume that government regulation will be without its faults?

Counselor [turning to Merchant]: Fair enough, but I want to hear more about the free market solution you're advocating. Be more specific. A market for personal information? Are you suggesting that we create property rights to personal data and then let them be traded in the market?

Merchant: Well, uh, basically yes, dear Counselor.

Counselor [turning to Economist]: But Economist, merely creating property rights in personal data says nothing about to whom that property is initially assigned, correct? So, let's say a citizen bought prodigious amounts of St. John's herb from a vendor last Friday.

---

33. EUGEN EHMANN & MARCUS HELFRICH, EG-DATENSCHUTZRICHTLINIE KURZKOMMENTAR [EU Data Protection Directive Commentary] art. 7 n.6 (1999).

34. *See* EU Data Protection Directive, *supra* note 29, at art. 7 (a).

35. *See id*. at art. 7 (b)–(f).

Which of them owns the "property" that is the knowledge of the citizen's purchase? And what precisely would such ownership entail?

Philosopher [jumping in excitedly]: Brilliant, my dear Counselor. The legal construction of a property right in personal information does not guarantee the individual much of anything. After all, the mere creation of property rights to bread doesn't mean that the poor are fed: it helps to give the poor the bread in the first instance. [Looking smugly at Merchant and Economist.]

Counselor: Well, Economist, in the market approach, who gets the property right in the first instance? [Economist scratches his chin.]

Economist: Well, if transaction costs are low, it may not matter . . .

Philosopher [interrupting]: Of course it matters! It must be the citizen. It is about her, isn't it? It is her dignity at stake.

Counselor [turning toward Philosopher]: But Philosopher, why?[36] Should I have plenary control over all information about me, such that even if I disserve the Queen by licentiousness or incompetence, no one in Atlantis should be able to speak about it, since it would somehow make use of my "property"? Why must the individual be given that property in the first place?[37] Is not personal data, created through social and commercial interaction, held in a sort of "joint authorship" between both citizens and merchants?[38] And if I

---

36. *See* RICHARD A. POSNER, THE ECONOMICS OF JUSTICE 234 (1981), at 233 (concluding that "[i]t is not clear why society should assign the property right in such information to the individual to whom it pertains").

37. Our point here is not that data collectors *should* be assigned the property rights to "jointly authored" personal data in the first instance. To the contrary, one of us has argued in picayune detail why it is more allocatively efficient (not to mention more respectful of human dignity) to adopt contractual default rules roughly equivalent to assigning the property right to the individual in the first instance. Rather, our point is that the *individual's* ownership of personal data is not self-evident. Thus, in a property approach, the central issue quickly becomes not whether to treat personal information as property, but whether and to what extent *the individual* should be the owner of such a proprietary right in the first instance.

One may also draw a parallel to the right of publicity. Just as celebrities are entitled to a proprietary right in their marketable identity in order to profit from their valuable public image, a reasonable argument can be made that all individuals should have the right to control and profit from the increasing commercial value of their everyday personal data. *See* J. Thomas McCarthy, *Melville B. Nimmer and the Right of Publicity: A Tribute*, 34 UCLA L. REV. 1703, 1711 (1987) ("[N]othing is so strongly intuited as the notion that my identity is mine – it is my property, to control as I see fit."); *see also* Jennifer L. Carpenter, *Internet Publication: The Case for an Expanded Right of Publicity for Non-Celebrities*, 6 VA. J.L. & TECH. 3 (2001); Rochelle Cooper Dreyfuss, *Warren and Brandeis Redux: Finding (More) Privacy Protection in Intellectual Property Lore*, 1999 STAN. TECH. L. REV. 8, ¶ 5 (1999); Laudon, *supra* note 6, at 102 (arguing that the property interest that celebrities have in their image should also be extended to the digital data images of ordinary individuals). *But see* Alicia M. Hunt, *Everyone Wants to Be a Star: Extensive Publicity Rights for Noncelebrities Unduly Restrict Commercial Speech*, 95 NW. U.L. REV. 1605 (2001).

38. *See, e.g.*, Froomkin, *supra* note 4, at 1521 (stating that under common law, absent a special duty of confidentiality, the "facts of a transaction belong jointly and severally to the

recall correctly the European philosopher John Locke, should I not credit the labor of Merchant who collected and exploited those data in the first place?[39] What do you say, Economist?

Economist [finishing scribbling some calculations on the back of an envelope]: Whether the property right should be assigned to citizens or the merchants raises difficult theoretical and empirical questions about which allocation best promotes allocative efficiency. There is some reason to think, however, that it would be most efficient to give citizens the property right in the first place.[40]

Counselor: Interesting. [Turning back to Merchant.] So is this what you seek when you champion the free-market approach? Shall I inform the Queen that your call for a market approach involves creating property rights in personal data and then assigning them to citizens in the first instance?

Merchant: Well, not exactly, dear Counselor.

Counselor: But what is the alternative? Granting the property right to you, Merchant? I buy medicinal herbs from you, and that fact you own? If I want to control that fact and keep it from the local gossip or employer, I must purchase it back from you?

Merchant [nervously]: Well, it would be in our interest to keep personal data confidential in the first place and share it only with our trusted business partners, who would offer only services and products that would improve your lifestyle. And of course, we wouldn't prevent you from using that fact yourself. We couldn't do that. We wouldn't own that fact *exclusively*.

Counselor: Now I am confused. If the property of personal information is not owned exclusively, then are you suggesting some sort of *commons* — not a typical stance for merchants.[41] What is the point of "propertizing" personal data only to deposit it immediately in the "commons" for the individual and merchant and perhaps others to use simultaneously? From a citizen's perspective, whether a merchant

---

participants"); Daniel J. Solove, *Conceptualizing Privacy*, 90 CAL. L. REV. 1087, 1113 (2002) (observing that "personal information is often formed in relationships with others" and rarely belongs to just one individual).

39. *See also* Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373, 1381 (2000); Seana Valentin Shiffrin, *Lockean Arguments for Private Intellectual Property, in* NEW ESSAYS IN THE LEGAL AND POLITICAL THEORY OF PROPERTY 138, 141 (Stephen Munzer ed., 2001) (rejecting claim that Lockean foundations support "strong, natural rights over most intellectual works").

40. The details regarding this proposition — based on an analysis of efficient default rules, which pay attention to extant preferences, the costs of sticking to an inefficient default distribution, and the costs of flipping into an efficient allocation — appear in Kang, *supra* note 4, at 1249–59.

41. Another possibility, which is not explored in the dialogue, is a form of joint ownership. One could imagine information about certain voluntary sexual relations falling into this category; no party can, so to speak, kiss and tell without every participant's agreement.

owns the property exclusively or just has plenary ability to process it matters little, doesn't it?

Merchant [befuddled]: Well, uh . . .

Philosopher [interjecting]: Dear Counselor, you have unmasked the fact that Merchant has no desire for anything besides the status quo. On the one hand, any official adoption of a market approach that initially assigns the property right to citizens would not be in his interest. On the other hand, calling for the opposite assignment would reveal publicly that notwithstanding Merchant's public relations campaigns, he has little genuine interest in promoting privacy. The confused status quo — an entitlement-anarchy — suits Merchant best. It makes little difference for data processors whether they own personal data exclusively or commonly. In either case, they can process the data as they will.

Counselor: Hmmm. What about you, Economist? If we implement a property-based market approach and assign the initial right to citizens, what happens then?

Economist: As I stated earlier, that may be the most efficient initial allocation. Market exchanges will then transfer that information to whichever party values it most, thereby achieving efficiency.

Counselor: Under this implementation — just to be clear — that initial assignment of property could not be taken away without the *consent* of the owner, right?

Economist: Yes, dear Counselor, as with any property.[42]

Counselor [looking at both Economist and Philosopher]: Now I am even more confused. How does your system [looking at Economist] differ from the one championed by Philosopher? Is this not the same as the "consent" necessary under the European Data Protection Directive? Consent as respecting dignity versus consent as respecting property, what is the difference?

2. Data Protection Regulations (or Intangible Property Regulations)

Philosopher [looking offended]: Dear Counselor, there remains a deep divide between the two approaches that superficial similarities should not paper over. For example, the EU Directive includes far

---

42. *Cf.* Guido Calabresi & A. Douglas Melamed, *Property Rules, Liability Rules, and Inalienability: One View of the Cathedral*, 85 HARV. L. REV. 1089, 1105 (1972) (categorizing different forms of initial entitlements depending on whether they are protected by property rules, liability rules, or rules of inalienability).

> In our framework, much of what is generally called private property can be viewed as an entitlement which is protected by a property rule. No one can take the entitlement to private property from the holder unless the holder sells it willingly and at the price at which he subjectively values the property.

Id.

more data protection regulations than just individual consent. *Inter alia*, the Directive commands judicial remedies for breach of data privacy rights, it entitles the individual to receive compensation in case of an unlawful processing of data, and it imposes sanctions for any infringement of data privacy regulations.[43] In addition, it also prescribes establishing supervisory authorities empowered to monitor and enforce data privacy laws.[44]

Counselor: I see. These additional regulations somehow remind me of our digital copyright discussions. Did we not do similar things to protect intellectual property — another type of information we are in the habit of calling "property"? Technologist, you've been typing away on that laptop the entire discussion. Anything to add?

Technologist [shutting down his instant messaging program and his web browser]: Uh, sorry . . . a lot of similarities between the privacy and property approaches because bits are bits, whether you call it "personal data" or "intellectual property." As Economist always says, information is intangible and non-rivalrous. In other words, you can't simply build a fence around your personal information to keep others away from it.[45] And although we notice when somebody has taken away our car, we usually have no way of knowing when somebody has taken our data (since it's non-rivalrous). And once info gets out in the clear, it's practically gone. You can't take control of it back.

Counselor: And how does that in any way respond to my question?

Technologist: The point is that self-help measures don't work so well with controlling bits in cyberspace. That's why we need all these regs. One could imagine pumping serious money and time into self-help through crypto. But that's unrealistic since personal data are created in everyday interactions, in public.[46] Finally, it's extremely tough to keep track of personal data in secondary transfers. In other words, even if the info is properly used by the first party, when that party conveys the info to party number two, it's hard for the individual to

---

43. EU Data Protection Directive, *supra* note 29, arts. 22–24. According to Article 22 ("Remedies"), Member States shall guarantee access to their courts for any breach of individual privacy rights. Details (which court or which branch of judiciary) are left to the Member States. According to Article 23 ("Liability"), Member States shall provide individuals with the right to compensation for damages suffered due to the unlawful processing of personal data. Article 24 ("Sanctions") requires Member States to lay down sanctions to be imposed on infringers of data privacy provisions. Again, the details of those sanctions (criminal provisions, civil penalties, or prosecution ex officio or on motion) are left to the Member States.

44. EU Data Protection Directive, *supra* note 29, at art. 28.

45. *But see* David Post, *Privacy, Property, and Cyberspace*, AM. L., Nov. 1997, at 98–99 ("[T]he possibility of constructing perfect fences around electronic information is far easier to conceive of on the electronic frontier than its physical counterpart.").

46. *See* Froomkin, *supra* note 4, at 1465 ("When solitude is not an option, personal data will be disclosed 'voluntarily' for transactions or emitted by means beyond our control.").

verify whether that second party is using the info in accordance with the license, permission, or authorization connected to that data. As a practical matter, once information is "out," forget about maintaining exclusive control over it.[47] If anyone has any doubt, ask the record labels about Napster and Kazaa. [Technologist touches a key on his laptop, minimizing his peer-to-peer program's window.]

Counselor: Kazaa? What is this you speak of? Something my teenage daughter would know about, but not me?

Technologist [turning off a vibrating cell phone]: Napster and Kazaa are examples of peer-to-peer networks that allow individuals to exchange files, music and video mostly, with others on the network. Our experience with copyright law shows that it isn't easy to protect property rights in a digital world. Legally recognizing some property right in info means squat — especially if the object of desire is a stream of ones and zeros — easy to store, copy, and distribute, as is the case with personal data. This is why in copyright law, we have loads of litigation[48] but have also pushed toward digital rights management ("DRM") technologies. And what's more, Hollywood's not banking only on self-help crypto; they've also gotten law on their side.

Counselor: Do you mean the notorious Digital Millennium Copyright Act?

Technologist: Bingo. The DMCA sets two prohibitions, one on circumventing tech measures used by copyright owners to protect their work and one on manipulating copyright management info. It creates new civil and criminal penalties for violating these provisions,[49] which are characterized as necessary to protect the exclusive rights granted by copyright.[50] Their purpose is to prevent a sort of digital arms race between those who crack DRMs and those who build

---

47. *See* Pamela Samuelson, *Information as Property: Do* Ruckelshaus *and* Carpenter *Signal a Changing Direction in Intellectual Property Law?*, 38 CATH. U.L. REV. 365, 369 (1989).

48. *See, e.g.*, A&M Records, Inc. v. Napster, Inc., 284 F.3d 1091 (9th Cir. 2002) (affirming a District Court's order to shut down Napster's website until it installed a new filtering system that prevented infringement of copyrighted musical works); Universal City Studios v. Reimerdes, 111 F. Supp. 2d 294 (S.D.N.Y. 2000) (enjoining defendant computer hackers from posting DeCSS, a computer program that circumvents an encryption system for DVDs and from electronically "linking" their site to others that post DeCSS). See also Paramount Pictures Corp. v. RePlayTV, Inc., 298 F. Supp. 2d 921 (C.D. Cal 2004), in which a lawsuit was filed by a number of television and film companies against SONICblue Inc. and its wholly owned subsidiary RePlayTV, Inc. The plaintiffs alleged that defendants' digital video recorder, ReplayTV 4000, violated copyright protections by enabling consumers to record digital copies of TV shows and movies and distribute them via the Internet to other ReplayTV customers.

49. *See* Copyright Act, 17 U.S.C. §§ 1201–02 (1976). For an introduction to the DMCA, see U.S. COPYRIGHT OFF., THE DIGITAL MILLENNIUM COPYRIGHT ACT OF 1998: U.S. COPYRIGHT OFFICE SUMMARY (1998).

50. U.S. COPYRIGHT OFF., *supra* note 49, at 3.

them.[51] So, there we have it, a beautiful example of "intangible property" regs — including statutory prohibitions, civil remedies, and criminal penalties — all implemented to provide something more than purely formal enjoyment of a property right over a stream of ones and zeros.

Counselor: I am trying to keep up with you and your lingo. Are you suggesting that the European regulatory apparatus (protecting personal data for dignity's sake) is similar to the American regulatory apparatus (protecting intellectual property for ownership's sake)?[52]

Technologist: Exactly. It's all about protecting the data. Whether it's a pop song or your shopping patterns, it doesn't really make a difference. If you want to fix privacy, you can't simply assign property rights in personal information (to the individual) and then call it a day. Trade-secret-like self-help measures through crypto won't hack it either. Take it from me, I'm the techie here. If for no other reason than to avoid an arms race between competing privacy-invading and privacy-enabling technologies, legislative intervention is necessary.[53] Law not only has to determine the level of data protection, but also must provide efficient means to maintain this level. I know I'll get in trouble with my fellow techies for saying this, but I'm just calling it as I see it.

Counselor: So, my confusion runs even deeper. When we started our conversation, I thought fundamental differences distinguished the dignity and the market approach. But they both *could* have starting points that give to the individual some "thing," [Philosopher winces] whether we call it a dignity right or a property right. And that "thing" allows an individual control over what happens to personal information.

Next, I thought we could locate some fundamental difference by focusing on the regulatory apparatus supporting and enforcing each approach. The dignity approach included many regulations, a virtue for Philosopher, a vice for Merchant. As Technologist just explained, however, a property approach *could* also require substantial regulatory apparatus for an owner to enforce effective control over intangible property.

So, in the end, am I to believe that the two core elements found in the *dignity* approach (individual consent and data protection apparatus) can also be the core elements of a credible *market* approach (initial allocation to the individual and intangible property apparatus)?

---

51. *See* Schwartz, *supra* note 31, at 849.

52 *Cf.* Jonathan Zittrain, *What the Publisher Can Teach the Patient: Intellectual Property and Privacy in an Era of Trusted Privication*, 52 STAN. L. REV. 1201 (2000) (exploring analogies between technological and regulatory protection of intellectual property and medical privacy).

53. *See* Kang, *supra* note 4, at 1245.

Can it be true that these two ways of thinking about privacy, supposedly so radically different in form, could turn out to be so remarkably similar in substance?[54]

B. Too Little Control

1. The Problem: Hard Choices

Philosopher: Counselor, your inclination to clump the two approaches obscures significant differences. For example, the market approach provides *too little control* over personal data. In the marketplace, personal data will be lost in the shuffle, with citizens making bad choices or being coerced into transactions from which they cannot walk away. Even if "property" rights — if we must call them that — in personal information are assigned to individuals initially, this assignment will not guarantee autonomous data-control.

Counselor: But why not?

Philosopher: Well, to use the rhetoric of the economists, citizens suffer from both *information asymmetry* and *power inequality*.[55] First, individuals might lack the necessary information to be able to make an autonomous decision. Often they are not even aware that their personal data are being processed. In other cases they do not know or do not understand the extent and purpose of data processing or the possibility of preventing it through contract.

Merchant: But we post privacy policies as part of our self-regulation initiative. It is within our voluntary code of ethics.

Philosopher: True, but they are cryptic or in small print no one reads, and subject to unilateral change. Further, an individual cannot easily determine the actual consequences of disclosure. A single piece of information might not be significant in the context of the actual contractual relationship. Yet, combined with other information or

54. To be clear, we are not contending that the *potential* convergence between the dignity and market approaches suggested by the Counselor must *actually* materialize. They could, of course, be radically different in the final implementation. But the same could be said of two approaches that are based on the *same* idea (compare a market approach that grants the initial allocation to the individual as compared to a market approach that grants the initial allocation to the merchant). Our rather modest point is that such convergence is quite possible and that the different forms of discourse do not necessarily produce significant divergence in practical result.

55. *See, e.g.*, A. Michael Froomkin, *Regulation and Computing and Information Technology: Flood Control on the Information Ocean — Living with Anonymity, Digital Cash, and Distributed Databases*, 15 J.L. & COM. 395, 493 (1996); Seth Safier, *Between Big Brother and the Bottom Line: Privacy in Cyberspace*, 5 VA. J.L. & TECH. 6 ¶ 94 (2000); Solove, *supra* note 4, at 1450–55; Cohen, *supra* note 39, at 1396–99 (raising various problems including present valuation, commensurability, and distributive justice).

transferred to a third party, the character or substance of the information changes.[56]

Merchant: Our citizens are not so stupid!

Philosopher [without missing a beat]: Second, there is power inequality. People who transfer ownership of their personal data might do so only because they lack sufficient bargaining power. Confronted with a take-it-or-leave-it situation, an individual may lack any practical ability to negotiate privacy terms. After all, the entire point of a form contract is to gain the efficiencies of standardization. Moreover, a company might be the only provider of the goods or services required. In order to obtain a certain benefit, the consumer has no choice but to accept the company's terms even if they require the disclosure of personal information as a necessary prerequisite. In this case, the consumer must click on the "yes" button or receive no service at all. This is why those who understand privacy as dignity counsel against propertization and instead suggest regulatory regimes, such as the EU's.

Counselor: I see. But Philosopher, the problems of information asymmetry and power inequality are not unique to the property approach, are they? Aren't these problems inherent to any approach that puts individual control at the heart of privacy? And would this not include the EU's approach?[57] Under the EU Data Protection Directive, consent by the individual justifies processing of personal data, correct?

Philosopher: Yes, it generally does.

Counselor: Perhaps I am being obtuse, but what is the practical difference between *consenting* to the processing of personal data within a regulatory regime and *licensing* some parts of my personal data within a property regime? In both cases, I exercise formal control over my data. In both cases, this exercise brings the benefits of flexibility and autonomy, but at the same time bears the real-world risk of power inequality and information asymmetry. Thus, the complaints

---

56. *See* Cohen, *supra* note 39, at 1398 ("A comprehensive collection of data about an individual is vastly more than the sum of its parts."); Froomkin, *supra* note 4, at 1501–05 (speaking of market failure caused by "myopic, imperfectly informed consumers").

57. EU Data Protection Directive, *supra* note 29, art. 7 ("Member States shall provide that personal data may be processed only if: (a) the data subject has unambiguously given his consent."); *see supra* notes 29–31 and accompanying text. *See also* Viktor Mayer-Schoenberger, *Generational Development of Data Protection in Europe*, in TECHNOLOGY AND PRIVACY: THE NEW LANDSCAPE 219, 234 (Philip E. Agre & Marc Rotenberg eds., 1997) ("Individual participation rights rank prominently among this directive's regulations. Accordingly, the directive lists individual consent as one of the legally accepted reasons for the processing of personal data . . . ."). Mayer-Schoenberger regards the focus on individual rights to be the main feature of the second and third generation of European data-protection norms (whereas the first generation took a functional look at data processing directly shaping and influencing the use of information-processing technology). *Id*. at 221–32.

about power inequality and information asymmetry apply to *both* property and regulatory approaches — do they not?

2. The Response: Fortifying the Individual

Philosopher: Dear Counselor, you are never obtuse. It is true that problems of information asymmetry and power inequality exist also within the dignity approach; however, the dignity approach makes stronger commitments to do something real, not just formal, about those matters. Consider again, for instance, what Europe has done.

The EU's regulatory approach responds to the problem of information asymmetry by establishing the requirement of *informed consent*. Article 2(h) of the Directive defines that "'the data subject's consent' shall mean 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."[58] The Directive has therefore created a duty to inform. According to Article 10 of the EU Data Protection Directive, the data processor must provide a multitude of information as to its own identity, the purposes of the processing, the recipients of the data, whether replies to the questions are obligatory or voluntary, the possible consequences of the failure to reply, and the existence of the right of access to and correction of the data.[59] The purpose of this notice is to "guarantee fair processing in respect of the data subject" by enabling the individual to give informed consent.[60] Consequently, in the case of incomplete or incorrect information, the consent of the data subject is deemed null and void.[61]

Informed consent requires not only that data processors provide the relevant information, but also that individuals are aware of the mode and the extent of data processing to which they are consenting. Article 7(a) of the EU Data Protection Directive therefore requires that the data subject has "*unambiguously*" given her consent to the processing of personal data.[62] It is generally understood that this requirement of unambiguity entails that consent must refer to a *specific* use of the data.[63] Individual consent to the processing of personal data therefore may never be construed as a general consent to all conceivable forms of data processing.[64] For example, one cannot sell one's

58. EU Data Protection Directive, *supra* note 29, art. 2(h) (emphasis added).

59. *Id*. at art. 10 ("Information in cases of collection of data from the data subject.").

60. *Id*.

61. ULRICH DAMMANN & SPIROS SIMITIS, EG-DATENSCHUTZRICHTLINIE KOMMENTAR [EU Data Protection Directive Commentary] art. 3, n.24 (1997).

62. *But see infra* note 92 (describing exceptions in art. 7(f)) (emphasis added).

63. *See* DAMMANN & SIMITIS, *supra* note 61, art. 7, n.4; Ehmann & Helfrich, *supra* note 33, art. 7, n.10.

64. *See, e.g.,* SPIROS SIMITIS, KOMMENTAR ZUM BUNDESDATENSCHUTZGESETZ [German Federal Data Protection Act Commentary] § 4a, n.74 (2003).

digital profile by simply giving a general waiver of all personal data collected by one's Internet Service Provider. The individual must be told what kinds of data are covered by the consent, what are the authorized purposes of data processing, and who are the legitimate recipients in the case of data transfer.

Counselor: Interesting. What about the power inequality matter?

Philosopher: The Directive, I concede, does not provide much guidance on that issue. It merely rules that consent is any *freely given* specific and informed indication of one's wishes.[65] But the Directive does not specify the particular circumstances under which consent may not be regarded as freely given.

Economist [interrupting]: What's more, the Directive allows consent to justify the processing of not only everyday data, but also *sensitive* data. European regulators, who praise themselves for protecting the dignity of their citizens, seem comfortable with the individual disclosing even her most intimate details such as political opinions, philosophical beliefs, or health information.

Counselor: Is this true, Philosopher?

Philosopher: Only partially. The Directive leaves it up to the Member States whether they want to prohibit the voluntary disclosure of sensitive data.[66] Take the example of genetic data, which are especially sensitive. In order to protect the individual against possible coercion, several European nations have prohibited employers and insurance companies from requiring the disclosure of genetic data. Furthermore, the laws prevent the receiving of such data *even when the individual voluntarily attempts to disclose the information*.[67]

---

65. EU Data Protection Directive, *supra* note 29, art. 2(h) ("'[T]he data subject's consent' shall mean 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.").

66. Article 8(1) of the EU Data Protection Directive, *supra* note 29, rules that "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." However, according to Article 8(2) this prohibition shall not apply where "the data subject has given his explicit consent to the processing of those data, *except where the laws of the Member State provide that the prohibition referred to in paragraph 1 may not be waived by the data subject giving his consent*" (emphasis added).

67. *See, e.g.*, ÖSTERREICHISCHES GENTECHNIKGESETZ [Austrian Law on Genetic Engineering], § 67 (1994). Other European countries also have laws forbidding the use of genetic data even when the data are disclosed voluntarily; see the Belgian Insurance Act of 1992, the Danish Insurance Act of 1997 (preventing insurance companies from using genetic information), and the Norwegian Law on the Medical Use of Biotechnology of 1998 (preventing both insurance companies and employers from using genetic information). For a comprehensive overview of European national laws, see Schweizerischer Bundesrat, Botschaft zum Bundesgesetz über genetische Untersuchungen beim Menschen [Swiss Executive National Council, Communiqué Regarding the Federal Law on the Genetic Testing of Humans], BBl. 2002, 7361, 7383–87.

See also European Convention on Human Rights and Biomedicine; Council of Europe, Convention for the Protection of Human Rights and Dignity of the Human Being with re-

Merchant: More parentalism, completely disregarding an individual's freedom to make sensible choices for himself!

Philosopher: Such total bans seem much more reasonable when we imagine what would happen if individuals could consent to such disclosure. Those with good genetic data would receive some better price[68] and would disclose voluntarily. All those who didn't would simply be presumed by insurers and employers to have bad genetic data. Thus, in effect, those who choose to disclose would also be making the decision for all those who would rather not.[69] Only an outright ban can avoid this predicament.[70]

Counselor: I see. Finally, I am starting to notice some meaningful substantive differences between a dignity approach and a market one. Please continue.

Philosopher [excitedly]: With pleasure, dear Counselor. Less drastic options can also be deployed in response to the power inequality problem. For instance, we can bar the conditioning of certain goods and services on the processing of personal data not required for the provision of such goods and services. We see concrete examples of this strategy in German data privacy law. Section 3(4) of the German Teledienstedatenschutzgesetz[71] states that a provider shall not condition teleservices upon the consent of the user to process her data if other access to teleservices "is not or not reasonably provided" to the user.[72] The same is true for telecommunication services according

---

gard to the Application of Biology and Medicine, Nov. 19, 1996, art. 12, Europ. T.S. No. 164*, available at* http://conventions.coe.int/treaty/en/treaties/html/164.htm.

68. *See generally* Varian, *Economic Aspects*, *supra* note 6, at chapter "Incentives Involving Payment" (no pagination in electronic copy).

69. *Cf.* Jerry Kang, *Cyber-Race*, 113 HARV. L. REV. 1131, 1193 (2000) (discussing potential inferences from the lack of certain signals, in the context of racial information in computer-mediated market transactions).

70. For the approach of absolute protection, see also Mayer-Schoenberger, *supra* note 57, at 233.

71. Teledienstedatenschutzgesetz [TDDSG] [Act on the Protection of Personal Data Used in Teleservices] (§ 3(4)) (1997) (F.R.G.) *translated at* http://www.iid.de/iukdg/aktuelles/fassung_tddsg_eng.pdf (Aug. 1, 1997) ("The provider shall not make the rendering of teleservices conditional upon the consent of the user to the effect that his data may be processed or used for other purposes if other access to these teleservices is not or not reasonably provided to the user."). "Teleservices" in the sense of this Act are all electronic information and communication services that are designed for individual use and are based on transmission by means of telecommunication.

Mediendienste-Staatsvertrag [MDStV] (§ 17(4)) (2002) (F.R.G.) [Media Services Convention] contains the same provision for media services. The main difference between teleservices and media services is that the latter are not designed for individual use, but are directed to the public. § 2(1) MDStV (defining media services as "services of information and communication in text, sound or picture addressing the public and being distributed without a conductor or using a conductor").

72. The ban refers only to the processing of functionally unnecessary data. Data required for the provision and pricing of teleservices to be processed without the consent of the individual concerned. § 5 TDDSG.

to section 95(5) of the German Telekommunikationsgesetz.[73] "Other access" is unavailable if none of the alternative services is of the same quality or if other companies offer only parts of the service at issue; moreover, other access to service is "not reasonably provided" either if the other service is significantly more expensive or if it requires significant additional time in order to make use of it.[74] Recently, the idea of forbidding the conditioning of services upon the consent of the individual was also introduced to U.S. law. According to the privacy provisions of HIPAA,[75] health care providers cannot deny services if an individual refuses to authorize the use or disclosure of protected health information.[76]

Counselor: I was right. Finally, here are some differences worth fighting about. Do you not agree, Economist?

Economist: Yes, dear Counselor, but I would not have you believe that only dignity-based regulatory regimes can respond to problems of information asymmetry and power inequality. For example, under Atlantis' unfair or deceptive trade practices ("UDTP") statutes,[77] unfairness can be based both on disproportionate bargaining power and on imbalances of knowledge.[78] These statutes cover such

---

73. Telekommunikationsgesetz [TKG] (2004) (F.R.G.) [Telecommunications Act; as amended as of June 22, 2004] *available at* http://www.datenschutz-bayern.de/recht/tkg.htm.

74. JOHANN BIZER, RECHT DER MULTIMEDIA-DIENSTE [Law of Multimedia Services] § 3 n.211 (Alexander Rossnagel, ed. 2003).

75. Health Insurance Portability and Accountability Act of 1996 (HIPAA), 45 C.F.R. §§ 160–164 (1996).

76. HIPAA states that a "covered entity may not condition the provision to an individual of treatment, payment, enrollment in the health plan, or eligibility for benefits on the provision of an authorization." 45 C.F.R. § 164.508(b)(4). For exceptions and for the HIPAA's distinction between consent and authorization, see DANIEL J. SOLOVE & MARC ROTENBERG, INFORMATION PRIVACY LAW 212–13 (2003).

77. For a comprehensive summary of UDTP codes, see JONATHAN SHELDON & CAROLYN L. CARTER, UNFAIR AND DECEPTIVE ACTS AND PRACTICES (5th ed. 2001). *See also* Federal Trade Commission Act 15 U.S.C. § 45 (2000) (prohibiting unfair methods of competition and unfair or deceptive acts or practices as well, but not explicitly providing for private remedies).

78. *See* Sheldon, *supra* note 77, at 160–63. State UDAP statutes provide enforcement either by the state Attorney General or by citizens through private rights of action. *See id*. at 81. State Attorney Generals have pursued state UDAP claims for privacy violations, even where the FTC has decided against action. Robert Gellman, *Enforcing Privacy Rights: Remedying Privacy Wrongs—New Models: A Better Way to Approach Privacy Policy in the United States: Establish a Non-Regulatory Privacy Protection Board,* 54 HASTINGS L.J. 1183, 1211 (2003) ("states have regularly been more effective in producing meaningful change than the FTC"). *See* Joel Reidenberg, *Enforcing Privacy Rights: Agency Enforcement and Private Rights of Action: Privacy Wrongs in Search of Remedies*, 54 HASTINGS L.J. 877, 888-89 (2003) (after the FTC declined to investigate the matter, ten states reached a settlement with Doubleclick for alleged violations of their UDAP laws, requiring changes in privacy practices to provide more information to consumers, including access to collected information). While infrequent, the FTC has pursued enforcement actions against "unfair" privacy violations causing unavoidable, substantial consumer harm unjustified by the benefits. Statement of Commissioner Mozzelle W. Thompson in ReverseAuction.com, Inc., File No. 0023046 (2000), *available at* http://www.ftc.gov/os/2000/01/reversemt.htm (improperly

different transactions as automobile sales, debt collection, door-to-door sales, and landlord-tenant matters.[79]

Counselor [looking to see Philosopher's reaction]: That is true.

Economist: Further, basic contract doctrines offer other responses. Simple refusal to recognize contract formation due to a lack of the meeting of the minds is one possibility. Other examples include duress, unconscionability (in both procedural and substantive forms), and public policy exceptions to enforcement.[80] Indeed, even property law features such public-minded exceptions notwithstanding the essential presumption of alienability.[81] Consider the various forms of pricing control (rent control, utility rate regulation, prescription drugs) and unwaivable warranties, such as the warranty of habitability.[82] One might even include certain laws that prohibit market-alienability,[83] such as those related to organ sales, as "property" laws that prohibit certain types of transactions.[84] In short, the market is not so simple-minded, as Philosopher suggests.

Counselor: Point well taken. Let me try to record some notes of my understanding so far.

---

obtaining consumer email addresses for deceptive use was "unfair" under FTC Section 5 authority). *See also* Stephen Calkins, *FTC Unfairness: An Essay*, 46 WAYNE L. REV. 1935 (2000). In addition to "unfair" behavior, the FTC has taken action against "deceptive" privacy-invasive behavior. *See* Jeff Sovern, *Protecting Privacy with Deceptive Trade Practices Legislation*, 69 FORDHAM L. REV. 1305, 1335 (2001).

79. *See* MARGARET C. JASPER, CONSUMER RIGHTS LAW 23–25 (1997).

80. *See generally* Julie E. Cohen, *DRM and Privacy*, 18 BERKELEY TECH. L.J. 575 (2003) (discussing public policy limitations on contracting).

81. *See* Margaret Jane Radin, *Market-Inalienability*, 100 HARV. L. REV. 1849, 1854 (1987) ("Market-inalienability negates a central element of traditional property rights, which are conceived of as fully alienable."). Free alienability is supposed to promote efficiency by allowing property to shift easily from lower to higher value uses. Richard A. Epstein, *Why Restrain Alienation?*, 85 COLUM. L. REV. 970, 972 (1985); JOSEPH WILLIAM SINGER, PROPERTY LAW 561 (1997).

82. *See* Catherine M. Valerio Barrad, *Genetic Information and Property Theory*, 87 NW. U. L. REV. 1037, 1083 (1992); Susan Rose-Ackerman, *Inalienability and the Theory of Property Rights*, 85 COLUM. L. REV. 931 (1985); *see also* JOSEPH WILLIAM SINGER, ENTITLEMENT: THE PARADOXES OF PROPERTY 74 (2000) (describing how certain property-related rights cannot be waived for public policy reasons that purport to protect one of the parties to the transaction or limit third-party externalities).

83. *See* Radin, *supra* note 81, at 1850 ("Something that is market-inalienable is not to be sold, which in our economic system means it is not to be traded in the market."). Various reasons are used to justify market-inalienability. *See id*. at 1909–14. The more important the object of commodification is to the individual's personhood, the greater the harm is to her personhood when she is coerced to commodify it. In order to prevent this harm, without having to face the difficulty of deciding in each individual case whether a transaction is voluntary or coerced, law bans a certain type of market transaction altogether. *See id*. at 1909–10.

84. *See, e.g.*, TEX. PENAL CODE § 48.02(b) (2002) ("A person commits an offense if he or she knowingly or intentionally offers to buy, offers to sell, acquires, receives, sells, or otherwise transfers any human organ for valuable consideration."); CAL. PENAL CODE § 367(f) (2001); *see also* National Organ Transplant Act, 42 U.S.C. § 274(e) (1984) (banning organ sales in interstate commerce).

First, both dignity and market approaches can privilege individual consent, with the market approach requiring the initial allocation of property rights to the individual. This is not to say that the market approach must make such an allocation, but it certainly can.

Second, both approaches can respond to the unique aspects of controlling intangible, non-rivalrous property that exist in digital domains by establishing the necessary legal enforcement apparatus.

Third, the problems inherent in making hard choices in a complicated world are not unique to the property approach; they arise within any regime that has individual consent at its foundation.

Finally, techniques that empower the individual confronted with hard choices are not restricted to a regulatory data privacy regime; they can appear in market approaches too. It appears, however, that the European approach has been more robust on this fortification.

C. Too Much Control

1. The Problem: Societal Overrides

Economist: Might I suggest that the dear Counselor has not sufficiently considered the costs of the so-called dignity approach? We must recognize the costs of granting to citizens too much control over personal data. Such costs include inefficiency, fraud, public endangerment, and chilling expression. Under the mantle of privacy, people can conceal unfavorable personal information to the detriment of their business and communication partners.[85] Granting exclusive control in personal data enables individuals "to manipulate the world around them by selective disclosure of facts about themselves."[86] People then keep quiet about their religious beliefs and political preferences, but then also try to hide their criminal activity, conceal a serious health problem from their employer, or mislead those with whom they transact. Privacy prevents accountability.[87]

---

85. *See* Anita L. Allen, *Privacy-as-Data Control: Conceptual, Practical, and Moral Limits of the Paradigm*, 32 CONN. L. REV. 861, 872 (2000).

86. RICHARD A. POSNER, THE ECONOMICS OF JUSTICE 234 (1981); *see also* FRED H. CATE, PRIVACY IN THE INFORMATION AGE 28 (1997) (arguing that privacy "facilitates the dissemination of false information").

87. For a feminist legal philosophical analysis of accountability and its relationship to privacy, see generally ANITA L. ALLEN, WHY PRIVACY ISN'T EVERYTHING: FEMINIST REFLECTIONS ON PERSONAL ACCOUNTABILITY (2003). Allen teases out various components of accountability, which, depending on the circumstances, could require the individual to "reckon or account in the sense of (1) reporting, (2) explaining, and (3) justifying acts and missions . . . (4) submit[ting] to sanctions and (5) maintain[ing] reliable patterns of behavior." *Id*. at 15. By controlling personal data, for instance, one could avoid "reporting" certain acts and omissions and thereby avoid that sort of accountability.

Merchant: I strongly concur. The power to conceal has huge economic consequences. Credit markets won't be able to distinguish between good and bad risks.[88] We also must assert our rights to freedom of speech. If merchants must keep mum about what we know about our customers, our freedom of expression has been limited.[89]

Counselor: Yes, Merchant, I do understand that an extreme position on privacy makes little sense. But you aren't suggesting that a property approach somehow avoids these hard questions, are you? For instance, if we create an exclusive property right in personal data *and* assign that property right in the first instance to the individual, the above complaints of "too much privacy" will arise in exactly the same way, will it not?

Merchant: [Remains silent . . . .]

Economist: Be that as it may, an approach that views every bit of personal information, however quotidian, to be wrapped up in some grand human right constrains too much how information is used in society. No sane society can allow individual control over personal data to always prevail.

Counselor: This much I understand. In addition to a "basic" rule in favor of individual privacy — whether we call it the requirement of consent or the initial allocation of the property right to the individual — categories of data and/or data situations have to be established that warrant departure from this basic rule. We need a list of cases in which society's needs override the individual's wants.[90]

Economist: And that is where a dignity approach seems irrationally romantic. It is insufficiently attentive to the justifiable processing of personal data when social welfare would thereby be increased.

2. The Response: Interest Balancing

Counselor: So, what do you say, Philosopher?

---

88. Various commentators resist or complicate the notion that more information is necessarily better. *See, e.g.*, Cohen, *supra* note 39, at 1408 (suggesting that data processing algorithms are "unforgiving and ungenerous . . . [leaving] little room, or tolerance, for randomness, idiosyncrasy, or mistake . . . learning effects and second chances."); Daniel J. Solove, *The Virtues of Knowing Less: Justifying Privacy Protections Against Disclosure*, 53 Duke L.J. 967 (2003).

89. *See* Eugene Volokh, *Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People From Speaking About You*, 52 STAN. L. REV. 1049 (2000) (addressing the conflict between free speech and information privacy in the context of the First Amendment and concluding that, under existing free speech law, it is not easy to justify expanding information privacy laws); *see also* Fred H. Cate & Robert Litan, *Constitutional Issues in Information Privacy*, 9 MICH. TELECOMM. & TECH. L. REV. 35 (2002) (arguing that the First Amendment limits governmental power in enacting and enforcing privacy laws that curtail expression).

90. *Cf.* ALLEN, *supra* note 87, at 22 (identifying "public need" as one ground of accountability).

Philosopher: Notwithstanding exaggerations to the contrary, a regulatory approach based on privacy as dignity need not be "irrationally romantic." For instance, the EU Data Protection Directive and its national implementing laws provide for societal overrides in various situations. Article 7 specifically identifies conditions under which data may be processed *even without the individual's consent*, for example, if processing is necessary for the performance of a contract, for compliance with a legal obligation, for the protection of the vital interests of the data subject, or for the performance of a task carried out in the public interest.[91]

Indeed, European laws feature general interest balancing provisions. Roughly speaking, these provisions strike a reasonable balance between the business interest of data controllers and the need for privacy of data subjects. For example, personal data may be processed if "processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject."[92]

Counselor: Excuse me, Philosopher, but what counts as "legitimate"? Everything? Nothing?

Philosopher: Consider, for instance, sections twenty-eight and twenty-nine of the German Federal Data Protection Act ("BDSG"),[93] which contain general interest balancing provisions similar to that of the Directive. These provisions cover a wide range of data processing performed by entities as diverse as address traders, credit reporting agencies, detective agencies, direct advertising companies, and market and opinion research institutes.[94]

In conducting this balancing test, German courts have consistently endorsed the public interest in the free flow of information. With regard to credit reporting, for example, the public interest in knowing the credit worthiness of business partners generally takes precedence over the individual interest in protecting the confidential-

---

91. EU Data Protection Directive, *supra* note 29, art. 7(b)–(e).

92. *See id*., at art. 7(f). Member States are free to adopt this general interest balancing provision or rather to specify in greater detail the circumstances in which personal data may be used or disclosed. However, most Member States also have merely implemented a general balance criterion into their national laws as set out in Article 7(f) of the Directive. *See* DOUWE KORFF, EC STUDY ON IMPLEMENTATION OF DATA PROTECTION DIRECTIVE 79 (2002), *at* http://europa.eu.int/comm/internal_market/privacy/docs/lawreport/consultation/univessex-comparativestudy_en.pdf.

93. Bundesdatenschutzgesetz [BDSG] (F.R.G.) [German Federal Data Protection Act], *translated at* http://www.bfd.bund.de/information/bdsg_eng.pdf (2003).

94. However, with regard to market and opinion research as well as direct marketing, the individual has a right to opt out of the processing of her data. *Id*. *at* § 28(4).

ity of one's personal data.[95] The balancing and exemption provisions of sections of the BDSG thus constitute the legal foundation for a credit reporting system that adequately serves the information interests of the market.[96]

Counselor: So, Economist, it appears that a "privacy as dignity" approach can, after all, recognize and implement "societal overrides" in a sensible way.

Economist: True, it would be an exaggeration to suggest that all regulatory approaches inevitably create some inflexible system that overprotects privacy.[97] But it bears repeating that the property regime can engage in such interest balancing even better. Such balancing has been explicitly recognized as a crucial element in property-like solutions.[98]

Counselor: So again, in the end, I see convergence. In both approaches we must specify categories of data processing in which what the individual wants is not what she gets. In the property approach, society must decide which kind of data may not be exclusively possessed by the individual, may be "fairly used" without the owner's permission, may be taken through "regulation" without compensation, or may be taken only with just compensation. Similarly, in the regulatory approach, society must decide which kind of data may be processed without the individual's consent. Of course, all this is nothing but common sense. No realistic system could be otherwise, correct?

[Economist, Philosopher, Merchant, and Technologist all nod their heads.]

---

95. *See, e.g.*, Bundesgerichtshof [BGH] [German Federal Supreme Court], Neue Juristische Wochenschrift [NJW], 39 (1986), 2505 (2506); BGH, NJW 56 (2003), 2904 (2905).

96. The leading German credit reporting agency, SCHUFA-Holding Corp., has information on sixty-two million people and has issued nearly seventy million reports in 2003. SCHUFA, SCHUFA BUSINESS REPORT (2003), *at* http://www.schufa.de/kennzahlen.html.

97. *But see, e.g.*, PAUL H. RUBIN & THOMAS M. LENARD, PRIVACY AND THE COMMERCIAL USE OF PERSONAL INFORMATION 60 (2002).

98. For instance, one of us has suggested a statutory solution that is arguably market-driven or property-like. That solution makes clear that, as a default matter, the individual's consent is not required if the data processing is functionally necessary to the cyberspace transaction that prompted the data collection. Kang, *supra* note 4, app. at 1287–94, § 4(a); for several other exceptions, see also § 6.

Other advocates of a property regime do not list specific exceptions, but nevertheless agree that those exceptions have to be made. Lessig, for example, draws an analogy to fair use in copyright law when emphasizing that individuals should not be in full control of all aspects of their personal data. *See* LESSIG, *supra* note 6, at 163. Rule and Hunter call what forms of personal data should not be under the exclusive control of the individual a "crucial matter." *See* Rule & Hunter, *supra* note 6, at 180. Shapiro and Varian, who also argue in favor of individual property in personal information, acknowledge that, of course, there is some information about individuals that is disclosed to serve a "public purpose." They suggest handling such issues on a case-by-case basis. *See* Shapiro & Varian, *supra* note 6, at ch. "Privacy," ¶ 7.

CONCLUSION

Counselor: [Bells in a faraway tower ring.] Our time is up. So what conclusion, if any, have we reached? Let me summarize what I have come to believe.

As all of you know, I have little patience for theoretical disputes that produce little substantive difference or that fail to illuminate practical questions. And, with all due respect to the two of you, Philosopher and Economist, I view much of your dispute to be academic. I simply do not care whether privacy is talked about in dignity or property terms. That dispute over language is abstract and, frankly, unhelpful. I concede that the language we use to describe privacy is not wholly unimportant, but in setting policy, it seems less significant than your pitched argument suggests.

Staying steadfastly away from matters of form, I will focus my comments to the Queen on substance. I see four basic steps in the analysis.[99]

1. *Initial entitlement*. Atlantis must decide who receives the initial entitlement of privacy in general cases. Whether we call it property or dignity matters little. Shall we favor the individual by assigning a dignity/property right in personal data to her? Or shall we favor the data processors and ostensibly the public by leaving personal data in the "commons?" As a general rule, I am inclined to favor the individual.[100]

2. *Fortifying the individual*. Since in most cases individuals will be able to give up these entitlements, we must make sure that they do so under fair circumstances. Individuals must know enough to make responsible choices.[101] And paradoxically, in certain cases, since for-

---

99. An omnibus approach would settle the matter generally for most categories of personal data, ranging from financial to medical to transactional. A sectoral approach would ask these questions separately for each category of information.

100. For justification of this assignment, in both efficiency and dignity terms, see Kang, *supra* note 4, at 1249–65.

The policy discussion between opt-in and opt-out can be reframed in "initial entitlement" terms. A legally binding opt-out approach places personal data in the commons, but provides the individual with an option to withdraw that personal data from the commons (without payment), at least for functionally unnecessary uses. By contrast, a legally binding opt-in approach grants the initial entitlement to the individual, at least for functionally unnecessary uses. Opt-in can exist in "market"-justified regimes, just as opt-out can exist in "dignity"-justified regimes. For example, the EU Data Protection directive envisions opt-out in certain circumstances. According to Article 14, the data subject shall have the right, "on compelling legitimate grounds relating to his particular situation," to object at any time to the processing of data relating to him, even if the data might lawfully be processed on the grounds of public interest, official authority, or the legitimate interests of a natural or legal person.

101. Relevant information would include the identity of the controller; the type of data processed; the purposes of the processing; and in the case of transfer of data, the recipients of the data. A different sort of knowledge that might be encouraged would arise from broad-

mal choice in the marketplace does not always improve the individual's actual lot, Atlantis may bar certain entitlement exchanges or renouncements.[102] In other words, an individual's decision *to allow data processing* cannot always be respected.[103]

3. *Societal overrides*. This point is in some ways the inverse of point 2. An individual's decision *not to allow data processing* cannot always be respected either. Rather, we have to establish reasonable exceptions to the general rule of individual control. To reach an agreement on the issue of societal overrides, we have to weigh the interests (commercial, law enforcement, etc.) of all concerned parties.[104]

4. *Legal enforcement apparatus*. Finally, we must determine the kind of legal apparatus necessary to enforce the norms established above. Self-help alone will be inadequate since we are dealing with information in a digital environment. Our prior experiences with intellectual property will prove useful, at least as an example.[105]

---

based education and debate about the values and countervalues of privacy. *See, e.g.*, Allen, *supra* note 31, at 735 (encouraging preaching and teaching about retaining privacy and consuming less of others' privacy).

102. Inalienability provisions can span a broad range:

- cannot process personal data under any circumstances (cannot ask, cannot offer);
- cannot price or condition services on "consent" to functionally unnecessary processing of personal data (effectively decouples the underlying transaction from the personal data transaction);
- cannot price or condition services on "consent" to functionally unnecessary processing of personal data unless reasonable alternatives, however defined, exist (requires a less than purely formal "choice," with "how much less" as a function of what counts as a reasonable alternative);
- regardless of any of the above, cannot "consent" to the waiver of certain rights regarding personal data, such as the right of access, correction, erasure, or blocking; this could also include the inalienable right to revoke prior consent.

103. This is not entirely radical. As Anita Allen points out, we already require certain types of inaccessibility notwithstanding an individual's desire to bare all. Consider laws against public nudity or public breastfeeding. *See* Allen, *supra* note 31, at 734.

104. Other, more concrete possibilities for societal overrides could include where:

- processing of data is necessary for the performance of a contract to which the data subject is a party;
- processing is necessary for compliance with a legal obligation to which the controller is subject;
- processing is necessary in order to protect the vital interests of the data subject;
- the data processed are generally accessible or the controller of the filing system would be entitled to publish them;
- processing of data is necessary for the conduct of scientific research;
- processing is necessary to avert threats to state security and public safety and to prosecute criminal offences.

105. Enforcement options might include:

- a right of every person to a judicial remedy for any breach of her privacy rights;

In each step there will be controversy, no doubt. But an abstract fight over dignity versus property does not seem especially helpful. I am not foolish enough to think that somehow serious privacy disputes, especially when large sums of money are at stake, will simply disappear because we ask these four questions. Still, from at least my untutored perspective, these basic questions focus us on a more useful inquiry, narrowing the areas of disagreement.[106]

Obviously, I was too optimistic when I had hoped today's meeting to be the end of the conversation. We shall meet another day, soon, to work through the details. On behalf of the Queen, Atlantis thanks you for your public-minded assistance. Good day.

[The Counselor exits. Lights dim.]

APPENDIX

A. Playwrights' Commentary

We were prompted to write this Socratic Dialogue because we thought that the current privacy debate unduly privileges form over substance. To make our case, it seemed natural to provide fictional spokespersons for different discourses and for them to try to explain to a no-nonsense Counselor what should be done. To avoid misreading or offense, we make clear that these characters are slight caricatures and that professional lawyers, lobbyists, and scholars could undoubtedly make better arguments than the ones presented in the dialogue.[107]

1. Clarifications

Potential, not actual, convergence. The dialogue demonstrates that whether one adopts dignity-talk or market-talk, neither framing necessarily dictates the way privacy will be experienced in the real world, by average folk. What is most important is where the power

- entitlement to receive compensation for damages as a result of the unlawful processing of personal data;
- imposition of state sanctions in case of unlawful processing of personal data;
- establishment of supervisory authorities or data protection commissioners, eventually with the power of investigation, intervention, or legal action.

106. We believe that these four basic questions serve as a useful new way to measure the state of privacy in any context. *Cf.* U.S. DEP'T. OF HEALTH, EDUC. AND WELFARE, SECRETARY'S ADVISORY COMMITTEE ON AUTOMATED PERSONAL DATA SYSTEMS, RECORDS, COMPUTERS, AND THE RIGHTS OF CITIZENS viii (1973) (providing a code of fair information practices); OECD, GUIDELINES GOVERNING THE PROTECTION OF PRIVACY AND TRANSBORDER FLOW OF PERSONAL DATA (Sept. 23, 1980), *available at* http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html.

107. *See supra* note 2.

over personal data is felt and exercised. This in turn depends less on the general discourse adopted than on the specific choices made within each discourse. The choice is not about dignity versus property; it is instead about strong or weak privacy. And the strength of that privacy can be usefully measured by the four variables outlined by Counselor at the dialogue's conclusion.[108]

There is nothing novel about the outcome of today's dialogue. It reflects the legal realist insight that the law on the books does not reflect the law in action. It also reflects the indeterminacy thesis and contestation of the public/private distinction from critical legal studies. Specifically, our story challenges the traditional understandings of the regulatory/property distinction,[109] which appears to blur when viewed from various vantage points.[110]

Not explicitly comparative. Although we made much of the EU's data protection directive, this piece should not be seen as an explicitly comparative piece. Most importantly, much of the "convergence" that Counselor teased out was possible by comparing an actual, existing directive (and its national implementing laws) to a hypothetical market approach that allocated property rights *to the individual* in the first instance. To be clear, such a property approach does not currently exist in the United States. Moreover, through this dialogue, we are not suggesting that the experience of privacy is identical across the Atlantic. Rather we believe the felt experience of privacy is greater on average in Europe than in the United States.

Recently, James Whitman has argued that privacy in Europe differs fundamentally from privacy in the United States because they come from two radically different cultural traditions. On the one hand, Continental "privacy" is really about "dignity" (or "personality"), concerned most with unauthorized portrayals of the self in mass media that involve losing face or honor.[111] On the other hand, Whitman argues, American "privacy" is really about "liberty," concerned most with state intervention into the sanctity of the home.[112] We believe that the difference is somewhat exaggerated.

For example, Whitman points to the restricted consumer credit reporting in France and Germany as evidence of the "honor-oriented, suspicious attitude towards . . . the free market" in Europe.[113] But

108. To recap, they are: (i) initial entitlement; (ii) individual fortification; (iii) societal overrides; and (iv) supportive legal apparatus.

109. *See* SINGER, *supra* note 82, at 78 ("Property and regulation are not opposites; they go hand-in-hand.").

110. Bearing this in mind, it should not shock us to hear the EU Data Protection Directive characterized by one commentator as "modeled on the property regime paradigm." *See* Safier, *supra* note 55.

111. *See* Whitman, *supra* note 23, at 1161.

112. *See id*. at 1161–62.

113. *Id*. at 1190–92.

credit reporting across the Atlantic, especially in Germany, does not differ as much as Whitman suggests. For example, the SCHUFA — the German equivalent to Equifax, Trans Union, and Experian — keeps files on sixty-two million German citizens, virtually the entire adult population. It issues nearly seventy million credit reports a year and assigns credit scores, not unlike its American counterparts.[114] The agency and its competitors are constantly expanding their fields of business by providing credit information for all kinds of transactions, such as leasing a car, renting an apartment, or getting cell phone service.

Indeed, one could argue that credit reporting *in the United States* is subject to more detailed privacy regulation.[115] In 1970 — when the risks of private data processing were not yet being discussed in Europe — the United States Congress passed the Fair Credit Reporting Act.[116] Regardless of its actual benefits in terms of protecting privacy,[117] this Act is one of numerous examples of American privacy legislation that is targeted — contrary to Whitman's suggestions — not at the state, but at private actors and at behaviors not always entirely conducted at home.[118]

In any event, whatever may be the actual magnitude and source of the cultural difference, our basic recommendation stands: for policymakers to focus not on "form" but on the four substantive questions outlined by Counselor at the dialogue's closing. In other words, just as a heated discussion between *dignity*-privacy and *property*-privacy was shown to be unhelpful, we question whether a debate between *dignity*-privacy and *liberty*-privacy will help Counselor to do her job. Obviously, differences in cultural and social values will lead societies to

---

114. *See* SCHUFA, *supra* note 96.

115. Credit reporting in Germany mainly is regulated by a general interest balancing provision. *See* BDSG, *supra* note 93.

116. Fair Credit Reporting Act of 1970, 15 U.S.C. §§ 1681–1681u (1994).

117. *See, e.g.*, Kang, *supra* note 4, at 1236–37 (suggesting that the FCRA would not much help the problem of information privacy in cyberspace transactions).

118. *See, e.g.*, Cable Communications Policy Act of 1984, 47 U.S.C. § 551 (2000); Video Privacy Protection Act of 1988, 18 U.S.C. § 2710 (2000). One could say that entertainment products are consumed at the home; however, videocassettes are rented in stores open to the general public, in plain view.

Just as Americans are not solely concerned about state violations of privacy, as evidenced by the statutes listed above, Europeans are also not indifferent to state processing of personal data. In fact, the latest transatlantic privacy clash — the conflict on the governmental use of air passenger data post 9/11 — suggests the contrary. According to the Aviation and Transportation Security Act, airlines are required to collect information on their passengers so that customs officials can check for security threats. Pub. L. No. 107–71, 115 Stat. 597 (Nov. 19, 2001). For a long time, Europe objected that the amount and kind of information its airlines were required to supply violated European privacy laws. In May 2004, the European Union approved an agreement with the United States to provide records of airline passengers to the American authorities. However, the European Parliament voted to refer the agreement to the European Court of Justice.

answer the four questions in different ways. But getting different answers depending on the society does not mean we are asking the wrong questions.

2. Discourse Matters

We also want to hedge the central point that form should give way to substance since discourse, of course, matters. Note that Counselor never says that discourse does not matter one iota; instead, Counselor goes only so far as to say that it is not wholly unimportant. Specifically, discourse might matter in three interrelated ways.

Cognitive. First, discourse might matter in terms of cognitive framing.[119] By using the metaphor or terminology of property, for instance, we may incline people to think a particular way about personal data, specifically to treat it more like their car than their soul.[120] Since we buy and sell cars, which are fully commodified, personal data that are likened to cars (in that both are property) may be seen in similar ways. By contrast, if we likened privacy's control over personal data to autonomy over one's body, then one might resist market exchange. Surely, the presumptions with which we engage in the debate will differ, both in terms of personal decisions and adjudications of conflicts. Selling Chevys seems like no big deal; selling body parts gives us some pause, at least at this cultural moment.

While the above explanation emphasized how a property-like conceptualization could encourage an individual to allow data processing in certain contexts, the opposite may be true. For instance, someone who views herself as hard-nosed and unsentimental may not see any "dignity" threat by merchant data collection practices; however, that same person might get indignant with the idea of someone appropriating her personal property (in the form of personal data) without compensation.

Political. Second, framing might affect politics. Different stakeholders have starkly different political objectives on privacy. For ex-

---

119. *See generally* SINGER, *supra* note 82, at 41–43 (discussing the significance of reconceptualizing public accommodation laws from equality terms, which posits a confrontation between property (ownership) and equality (antidiscrimination), to property terms, which posits a confrontation between two forms of property (ownership and easement)).

120. *See* Litman, *supra* note 8, at 1295–1301 (suggesting that a property model encourages the sale of personal data); Julie E. Cohen, *Lochner in Cyberspace: The New Economic Orthodoxy of "Rights Management,"* 97 MICH. L. REV. 462, 481 (1998) (suggesting that terms such as contract, market, and property can have "talismanic significance" to some); *see also* Cohen, *supra* note 39, at 1391 ("[P]roperty rhetoric may seem to privilege certain choices above others. Recognizing property rights in personally-identified data risks enabling more, not less, trade and producing less, not more, privacy."). *See generally* SINGER, *supra* note 82, at 83–84 (providing catalog of rhetorical functions served by the concept of "owner" of property).

ample, commercial interests keen on keeping the flow of personal data unrestricted will rationally deploy whatever discourse suits their objectives. That is why Economist is so heavily supported by Merchant when Economist proposes market-like solutions to privacy problems, even though Merchant does not in fact seek any clear property-like solution to the present contest over privacy.

As another example, consider what a libertarian might accept in terms of privacy regulation. If framed as a protection of a property right to personal data, she may embrace such regulation, just like she would support laws that prohibit theft or trespass. By contrast, if framed as government meddling in private party transactions to promote some parentalistic notion of "dignity," the libertarian might recoil.

Developmental. If privacy is essentially about satisfying an individual's preferences about the flow of personal data, we must consider how these preferences are created and changed by culture. It is shortsighted and reductionist to take them as exogenous. By stepping back, we see that the manner in which society (perhaps through law) frames privacy (in either market or dignity terms) can have symbolic value — a public statement about privacy's unspecial/special, fungible/unique value to the individual and her community. In turn, this framing can produce a positive feedback loop in the preference structure of individuals who live within that society. If we characterize privacy as property, then over time we may as a people come to adopt the preferences consistent with that analogy.[121] By contrast, if we characterize privacy as dignity, then, as before, our preferences might evolve accordingly.

In at least the above-mentioned ways, discourse *might* matter. But then again, it might not matter much at all. Take the example of European data privacy law: even though European law is touted as adopting the dignity approach to privacy, we see Europeans happy to use bonus cards and frequent traveler programs to receive discounts. They do not seem especially hesitant to disclose personal data in exchange for a free e-mail service or the chance to take part in a lottery. They are willing to sell their privacy for a couple of euros, as are Americans for a couple of dollars.[122] Consider, as another example, that the Ger-

121. *Cf.* MARGARET JANE RADIN, CONTESTED COMMODITIES 79–84 (1996) (suggesting that if personal characteristics and attributes are perceived as things that can be owned and disposed of, like ordinary objects of daily life, this also affects our personhood and our understanding of ourselves).

122. *See* Spiros Simitis, *Auf dem Weg zu einem neuen Datenschutzkonzept* [On the Way to a New Conception of Data Privacy], Datenschutz und Datensicherheit [DuD], 24 (2000), 714 (721) (warning about the increasing commercialization of personal data and pointing out that normally it does not take more than some "promotional gifts" or payment to get the necessary consent to data processing by the individual concerned).

man right to personality, once a "purely idealistic concept of personality rights,"[123] is slowly transforming into a property right.[124] Of course, this could simply demonstrate the imperialism of commodification rhetoric. Even so, that means that in American culture, we cannot suppose that a privacy solution adopted with the rhetoric of dignity will inevitably lead to some privacy-protective end result.

B. Deleted Scenes

Finally, for pacing and complexity reasons, the dialogue does not address various significant privacy issues. For example, there is no discussion about government processing of personal data, which has become especially significant in the United States after 9/11. It is plausible that dignity-talk might resist massive government profiling of its citizens more strongly than property-talk. In addition, we cut the following scenes. But we think there's value to them, so we include rough outlines for your consideration. Think of them as the director's cut in the enhanced DVD version of the movie.

1. The Dispute about P3P

The Platform for Privacy Preferences ("P3P"), as described by its advocates, is an industry standard "providing a simple, automated way for users to gain more control over the use of personal information on Web sites they visit."[125] P3P makes the privacy standards of websites available in a uniform, machine-readable format and enables browsers to compare those standards to the consumer's own set of privacy preferences.[126]

Whether P3P is a privacy-enhancing technology ("PET") or privacy-invading technology ("PIT") is disputed. On the one hand, Larry Lessig welcomes P3P as digital ball bearings in the marketplace for personal data, which will enable informed and autonomous consumers to negotiate and assert proprietary interests in personal data automati-

---

123. HORST-PETER GÖTTING, PERSÖNLICHKEITSRECHTE ALS VERMÖGENSRECHTE [Personality Rights as Property Rights] 54 (1995).

124. In contrast to the American right of publicity, German law widely rejected a commercial character of the personality right. However, the market took a different path — commercializing the name and likeness of celebrities. As a result, the German Supreme Court is gradually transforming the personality right into a property right. *See, e.g.*, Bundesgerichtshof [BGH] [German Federal Supreme Court], Neue Juristische Wochenschrift [NJW], 53 (2000), 2195 (ruling that the personality right does not only protect immaterial but also commercial interests and that, in the case of succession, the commercial elements of the right are transferred to the heirs).

125. *See* Platform for Privacy Preferences (P3P) Project, What is P3P? *at* http://www.w3.org/P3P/#what (last visited Dec. 4, 2004).

126. *Id*.

cally and efficiently.[127] On the other hand, Marc Rotenberg regards P3P as an "invitation to reject privacy"[128] that is intended to displace a privacy-protective regulatory regime in the name of formal choice. Although its supporters claim that P3P enhances individual privacy rights, Rotenberg contends that it will only lower the level of privacy protection.[129]

In the dialogue, we thought about entering this debate not to engage the substantive merits of P3P but merely to demonstrate that P3P should not be exclusively aligned as an incident to a "property" approach to privacy. The purpose of P3P is to support individual determination about whether or not to disclose personal data. And we have seen that individual determination is the essential element of both market and dignity-based privacy regimes. Accordingly, the idea of computer-facilitated agreements can be central to both property and regulatory regimes.

Our point is not that P3P actually enhances privacy. This depends on the design of data protection regulations generally (which influence background knowledge and power) and on the design of P3P specifically.[130] We agree with Rotenberg that it would be simplistic to assume that P3P could provide some magical technological fix to all relevant privacy concerns. At the same time, we do not rule out the possibility that P3P-like implementations might become one valuable element among others in an ideal solution set.

2. The Skeptic

The role of Skeptic would have been to question one of the fundamental assumptions held by both Economist and Philosopher: the privacy-control paradigm. According to Alan Westin's frequently quoted formulation, "[Privacy is] the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others."[131] Most information privacy scholars either directly cite this definition[132] or use

127. *See* LESSIG, *supra* note 6, at 160–61 (arguing that P3P provides the technical support for the establishment of a property regime of data privacy in which individuals may exercise choice, negotiate, and obtain value).

128. Rotenberg, *supra* note 31, at ¶ 89.

129. *See id*. at ¶ 90.

130. Consequently, European data privacy scholars do not reject P3P entirely but consider it as one possible future element in a concept of self-protection in data privacy. See, for example, Alexander Roßnagel, *Konzepte des Selbstdatenschutzes* [Concepts of Self-Protection in Data Privacy], *in* HANDBUCH DATENSCHUTZRECHT [Data Protection Law Handbook] ch. 3.4 ¶ 53 (Alexander Roßnagel ed., 2003) (stating that P3P has yet to be developed into a "true communication standard").

131. ALAN F. WESTIN, PRIVACY AND FREEDOM 7 (1967).

132. *See* Basho, *supra* note 7, at 1509; Solove, *supra* note 4, at 1445.

substantially similar definitions, consistently embedding the idea of control into the core.[133] The U.S. Supreme Court has also supported this view and suggested that "both the common law and the literal understandings of privacy encompass the individual's control of information concerning his or her person."[134] *Arguably, it is this focus on "control," whether viewed in terms of individual consent or property ownership, that creates the similarities in substance notwithstanding the differences in form*. To make this point, we imagined Skeptic saying something like this:

> **Skeptic** [addressing Counselor and the other characters]: Any system that tries to promote individual control over data will inevitably confront the fundamental questions you have termed "hard choices" and "societal overrides." Therefore, your dispute between regulatory and property approaches within the individual control paradigm misses the larger point. We must shift to some other privacy paradigm. Because both regulatory and property approaches are grounded in individual control, they will, in the end, provide only formal, inadequate protection.

In American legal scholarship, we have recently seen some privacy scholars contest this conceptualization of information privacy.[135] For example, Anita Allen argues that privacy should be defined as the "degree of inaccessibility of a person or information about her to others' five senses and surveillance devices."[136] Understood this way, it

---

133. *See* Rochelle Cooper Dreyfuss, *Warren and Brandeis Redux: Finding (More) Privacy Protection in Intellectual Property Lore*, 1999 STAN. TECH. L. REV. 8, ¶ 5 (1999) ("[P]rivacy means control over personal information."); Fried, *supra* note 18, 482 (1968) ("Privacy is not simply an absence of information about us in the minds of others; rather it is the control we have over information about ourselves."); Froomkin, *supra* note 4, at 1463 ("I will use 'informational privacy' as shorthand for the ability to control the acquisition or release of information about oneself."); Kang, *supra* note 4, at 1266 ("Recall that control is at the heart of information privacy."); LESSIG, *supra* note 6, at 143 ("Privacy . . . is the power to control what others can come to know about you."). Allen challenges this unanimity in definition, especially for philosophers working on privacy outside the cyberspace context. *See* Allen, *supra* note 85, at 866–87 (preferring a definition of privacy as factual condition of accessibility to other's senses and surveillance).

134. United States v. Reporters' Comm. for Freedom of the Press, 489 U.S. 749, 763 (1989).

135. *See* Allen, *supra* note 85, at 868 (stating that control is neither sufficient nor necessary for privacy); Schwartz, *supra* note 31, at 821 (arguing that privacy-control has proved to be a deeply flawed principle); *see also* Paul M. Schwartz, *Charting a Privacy Research Agenda: Responses, Agreements, and Reflections*, 32 CONN. L. REV. 929 (2000).

136. Allen, *supra* note 85, at 867. She states that "[t]he best conceptual reason for rejecting characterizations of privacy that emphasize control may be that control over personal data appears to be neither necessary nor sufficient for states of privacy to obtain." *Id*. This

is easy to see how one can freely exercise choice over personal data (privacy understood as control) in ways that diminish privacy (privacy understood as inaccessibility). To continue in the form of dialogue:

> **Skeptic** [sharply]: Look at our modern "culture," look at all these reality-TV shows, blogging, and live broadcasting of mastectomy and birth. And think of the public exhibition of sexual acts and fantasies, the installing of publicly accessible webcams in bedrooms and living rooms, and so on. How can you believe that privacy should be about individual control if you look at all these individuals who are exercising their control only to transform themselves into commercialized entertainment packages to satisfy their own exhibitionism and other people's voyeurism?[137]
>
> **Counselor**: It does seem to do some violence to the word "privacy" to suggest that someone who exposes herself naked nonetheless has "privacy" simply because she is exercising her free will. But what is the alternative? Can we construct some useful notion of privacy that abandons individual determination over personal data?
>
> **Merchant** [stunned]: An invitation for even more parentalism, I dare say!
>
> **Philosopher**: This time I must agree with the Merchant. Individual control has been the center of privacy from time immemorial. I agree that purely formal control is of little value, but that does not mean that the fundamental concept should be abandoned. Even Europeans have assigned crucial importance to this element within their data privacy regimes.

---

argument, however, suffers some circularity since it presupposes a definition of privacy that is not control-centered. Put another way, this argument amounts to: privacy-as-control should be rejected because it is neither necessary nor sufficient to produce privacy-as-inaccessibility.

137. For a new dimension of voyeurism, see Amy Harmon, *Smile, You're on Candid Cellphone Camera*, N.Y. TIMES, October 12, 2003, at WK3 (describing the proliferation of cellphone photography in public). *See also* ALLEN, *supra* note 87, at 35 (discussing voluntary exhibitionism).

> **Skeptic**: Well, even if we do not abandon individual control entirely, we nevertheless must question its status as the leading paradigm. I recommend that we move towards a "constitutive conception of privacy."

A constitutive theory of privacy could mean many different things. It would surely deemphasize the role of individual control, which Paul Schwartz has called a "deeply flawed principle"[138] that springs an "autonomy trap"[139] (what we identified as "hard choices"[140]). Julie Cohen has also pointed out the narrow ways in which we tend to understand "freedom of choice" as choice exercised solely in the marketplace, not recognizing that "[t]he design of markets, and whether to delegate resolution of particular questions to them, are themselves choices."[141] It would also likely establish some guidelines — whether framed as rules or standards, implemented through procedural and/or substantive reform — on the amount of privacy (appropriately defined) that best achieves some set of perhaps conflicting goals, such as human flourishing, autonomy, democracy,[142] equality, or accountability. Examples can be found in the work that has been dubbed the "New Privacy."[143]

If confronted with some such constitutive theory from Skeptic, the hard-nosed Counselor would aggressively question whether such a reconceptualization remains more form than substance. For example, Schwartz suggests that constitutive privacy involves "a matter of line drawing along different coordinates to shape permitted levels of scrutiny."[144] The function of privacy norms is not to build "data fortresses" that isolate personal information in some absolute sense[145] but to create "shifting, multidimensional data preserves that insulate per-

---

138. Schwartz, *supra* note 31, at 821.

139. *Id*. at 821–28.

140. Spiros Simitis, one of the leading privacy scholars in German law, pointed to these problems in an American law review as early as 1987. Spiros Simitis, *Reviewing Privacy in an Information Society*, 135 U. PA. L. REV. 707 (1987). He calls it "chimerical" to assume that effective protection of privacy can be accomplished by simply entrusting the processing decision to the person concerned. *Id*. at 736. For Simitis, the assumed control and interference opportunities of individuals are merely "fictitious" because "hospital patients, bank customers, and employees cannot determine the proper data processing conditions, even though their consent to disclosure of information is required." *Id*. at n.128, and accompanying text.

141. Cohen, *supra* note 39, at 1399.

142. *See* Paul M. Schwartz, *Beyond Lessig's Code for Internet Privacy: Cyberspace Filters, Privacy Control, and Fair Information Practices*, WIS. L. REV. 743, 761 (2000).

143. *See* Paul M. Schwartz & William M. Treanor, *The New Privacy*, 101 MICH. L. REV. 2163 (2003) (reviewing JOHN GILLIOM, OVERSEERS OF THE POOR: SURVEILLANCE (2001)) (identifying the works of Julie Cohen, Priscilla Reagan, Paul Schwartz, and Daniel Solove).

144. Schwartz, *supra* note 31, at 834.

145. *Id*.

sonal data from different kinds of observation by different parties."[146] Counselor would question whether creating such contextual shields through nuanced applications of fair information practices and adopting combinations of "disclosure and non-disclosure rules for the same piece of information"[147] would be much different, in practice, from the inquiries regarding "hard choices" and "societal overrides."

In this brief discussion, we are not attempting any serious analysis of the merits of an alternative conception of privacy. Rather, our modest goal has been to flesh out Skeptic's purpose — to argue that the convergence between the supposedly polar opposite "dignity" and "property" approaches is caused by adopting the same definition of privacy, which centers on individual control over personal data. Accordingly, the more interesting conversation in future theoretical work on information privacy, we predict, will not be dignity versus property, but individual control versus something else.

We hope you enjoyed the show. If the reviews are good, perhaps we will consider a sequel.

146. *Id*.
147. *Id*. at 835.