PROPERTY AS CONTROL: THE CASE OF INFORMATION

*Jane B. Baron**

Cite as: Jane B. Baron, *Property as Control: The Case of Information*, 18 MICH. TELECOMM. TECH. L. REV. 367 (2012), *available at* http://www.mttlr.org/voleighteen/baron.pdf

INTRODUCTION

If heath policy makers' wishes come true, by the end of the current decade the paper charts in which most of our medical information is currently recorded will be replaced by networked electronic health records ("EHRs"). Integrated, longitudinal EHRs will help doctors coordinate care across time and across specialties, enable patients and those who treat them to access relevant information wherever it is needed, and facilitate the creation of population health data that can be used to improve the health of all.[1] Although EHRs represent a substantial improvement over fragmented, geographically dispersed, illegible, and uncoordinated paper records, they pose new dangers as well. Like all computerized records, networked EHRs are difficult to secure, and the information in EHRs is both particularly sensitive and particularly valuable for commercial purposes. Sadly, the existing

* I. Herman Stern Professor of Law, Temple University Beasley School of Law. Thanks to Alice Abreu, Rob Bartow, Richard Baron, Julie Cohen, Craig Green, Rick Greenstein, Dave Hoffman, Sharona Hoffman, Gregory Mandel, Andrea Monroe, David Post, Mark Rothstein, Henry Smith, Sandra Sperino, and Nicolas Terry for comments on earlier drafts. Thanks also to Meghan Kenney and Olivia Jolly for research assistance. All errors are mine.

1. *See infra* notes 17–41 and accompanying text.

federal statute meant to address this problem, the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"),[2] is probably inadequate to the task.[3] Thus, the information in EHRs is as vulnerable as it is valuable.

Although medical information is in several ways distinctive, in many important respects such information is but a subset of "information" more generally, and the problems raised by EHRs instantiate a larger set of problems posed by the collection of information about individuals in cyberspace.[4] As is now well known, our digital trails allow the technologically sophisticated to assemble an uncannily accurate picture of our preferences, interests, economic status, political views, and consumption patterns. Sometimes the use of this picture can be beneficial, helping us get what we want more quickly and in more tailored ways, but, as is the case with medical information, the data collected about us can be dangerous. It can be used to deny us jobs or credit, to embarrass us, or to harass us.[5]

Health law, privacy, and intellectual property scholars have all suggested that the river of information created by integrated, networked EHRs and other data systems must somehow be controlled,[6] and many of these scholars have considered whether "property" might provide such control.[7] If

2. Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. No. 104-191, 110 Stat. 1936 (codified as amended in scattered sections of 18, 26, 29, 42 U.S.C.); *see also* HIPAA Security Rules, 45 C.F.R. §§ 164.302–.318 (2011)(specifically § 164.306, security measures generally; § 164.308, administrative safeguards; § 164.310, physical safeguards; § 164.312, technical safeguards; § 164.314, organizational requirements; and § 164.316, policies and procedures and documentation requirements).

3. *See infra* notes 42–46 and accompanying text.

4. As is developed *infra* notes 39–57 and accompanying text, medical information is meaningfully different from personal information collected in cyberspace, if for no other reason than that medical information is "confidential" and therefore subject to special duties that do not apply to other information. DAVID A. ELDER, PRIVACY TORTS § 2:6 (2011). But to the extent that even "confidential" information is only imperfectly protected, it shares many features in common with "ordinary," non-confidential personal information.

As a general matter, it is important to distinguish between "deidentified" information on the one hand and information that can be linked directly to an individual on the other. Deidentified information is "information that has been altered to remove certain data elements associated with an individual." Mark A. Rothstein, *Is Deidentification Sufficient to Protect Health Privacy in Research?*, 10 AM. J. BIOETHICS 3, 3 (2010). Deidentified information poses fewer risks for individuals than identified information. *Id.*

5. For two vivid accounts of the general process of data collection, see DANIEL SOLOVE, THE DIGITAL PERSON 13–26 (2004), and Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193, 1198–99 (1998).

6. *See, e.g.*, M. Ryan Calo, *The Boundaries of Privacy Harm*, 86 IND. L.J. 1131, 1134 (2011) (describing privacy harms as "the loss of control over information about oneself or one's attributes"); Julie E Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373, 1379 (2000) ("Data privacy advocates seek . . . to guarantee individuals control over their personal data."); Jessica Litman, *Information Privacy/Information Property*, 52 STAN. L. REV. 1283, 1286 (2000) ("[A]ctual control [of information] seems unattainable.").

7. *See, e.g.*, Mark A. Hall, *Property, Privacy, and the Pursuit of Interconnected Electronic Medical Records*, 95 IOWA L. REV. 631 (2010) (suggesting that patients be allowed to license rights to medical information for purposes of stimulating market development of

individuals had property rights in the information collected about them, then arguably that information could not be used without their consent.[8] Thus, some assert that by granting individuals property rights in the medical and other information collected about them, the law can prevent the more dystopian consequences of our wired world.[9]

The notion that property might help solve the problem of uncontrolled information was the subject of intense consideration over a decade ago,[10] but then interest somewhat waned. Increasing use of and support for EHRs has recently generated new proposals for the propertization of health information.[11] I leave to others the question whether these proposals adequately address the health and other assorted public policy issues raised by EHRs.[12] This Article focuses instead on whether the sophisticated, qualified ownership regimes scholars have propounded are appropriately characterized as "property" at all.

The Article's principal thesis is that arguments over the control of rights in personal information test contemporary understandings of what property is and reveal fault lines in modern property theory. If property rights exist at

---

EHRs); Edward J. Janger, *Privacy Property, Information Costs, and the Anticommons*, 54 HASTINGS L.J. 899 (2003) (exploring the possible costs and benefits of a regime of "muddy property rules" for personal information); Paul M. Schwartz, *Property, Privacy, and Personal Data*, 117 HARV. L. REV. 2056 (2004) (proposing a five-element model for propertized personal information).

These proposals are by no means uncontroversial. *See, e.g.*, Barbara J. Evans, *Much Ado About Data Ownership*, 25 HARV. J. L. & TECH. 69 (arguing that property rights might merely replicate the unsatisfying framework of patient protections already available under HIPAA); Marc A. Rodwin, *The Case for Public Ownership of Patient Data*, 302 J. AM. MED. ASS'N 86, 87 (2009) (arguing that property rights create a danger of an anti-commons that could make the cost of collecting population health data prohibitive); *see also* Cohen, *supra* note 6, at 1391; Pamela Samuelson, *Privacy as Intellectual Property*, 52 STAN. L. REV. 1125, 1136–46 (2000) (challenging the effectiveness of a property regime).

8. Pamela Samuelson, *A New Kind of Privacy: Regulating Uses of Personal Data in the Global Information Economy*, 87 CAL. L. REV. 751, 771 (1999) (book review) ("Propertizing personal information would . . . give members of the public some control, which they currently lack, over the traffic in personal data."). *But see id.* at 772 (expressing reservations about this proposal). To use the famous Calabresi and Melamud formulation, personal information would be protected by a "property" rather than a "liability" rule. *See infra* notes 60–62 and accompanying text for the development of this idea.

9. Of course, "property" is not the only legal device by which information might be controlled. Intellectual property, privacy, contract, and tort represent other possibilities. On these alternatives, see *infra* notes 59 and 66.

10. *See* Symposium, *Cyberspace and Privacy: A New Legal Paradigm?*, 52 STAN. L. REV. 987 (2000).

11. *See, e.g.,* Hall, *supra* note 7; *see also* Edmund Haislmaier, *Health Care Information Technology: Getting the Policy Right*, THE HERITAGE FOUND. (June 16, 2006), http://www.heritage.org/research/reports/2006/06/health-care-information-technology-getting-the-policy-right.

12. For a description of the wide range of these issues, see *infra* Part III.A.

all in "dephysicalized,"[13] digitized information, those rights are unlikely to be consolidated in a single person, to operate *in rem*, to grant owners significant powers to exclude, or to be standardized—qualities that, in the eyes of some, are required of true "property" interests. Claims of ownership to personal information also raise questions about whether property is the right rhetorical frame in which to consider the problem of information that is deeply connected to people's selves. Finally, propertization claims assume a closer connection between property and control than is either realistic or desirable in an interconnected world. It is likely that, at the end of the day, individuals will as a matter of policy be granted some rights to control some of their personal information, but those rights will not follow from anything in property's "nature."

Part I introduces the control issues raised by EHRs specifically and by the collection of personal information more generally, and then examines the arguments for using property as a device to control information. Discussions of property-as-control tend to adopt an excessively thin notion of property, focused on alienability. While under traditional property principles alienability is valued highly and restraints on alienation are disfavored, in the case of information, alienability is almost always seen as problematic.[14] To solve this problem, we could customize the alienability of property rights in personal information in ways that maximize individuals' powers of control while minimizing economic and moral dangers. But the rights produced by such customization might not look all that much like property rights. Tailored, customized rights will not easily be standardized and may thus fail to convey the information that some property theorists regard as essential to a working property system. To the extent that individuals might hold relation-specific "bundles of rights" against different parties in the information chain, their rights would lack the *in rem* quality that some believe distinguishes property from other legal rights. The debates over whether information property provides control thus test extant definitions of property.

Part II explores the connection between the loss of control over information and concerns about the "self." It questions whether property is the best frame in which to talk about medical and other personal information, i.e., whether, rhetorically, we should treat information about the self as a commodity. It questions also whether we can avoid a property frame. If commodification of the self is troubling, transferring the propertied self from invisible, commercial data aggregators to visible, embodied individuals does not solve the problem. But, I argue, when we see others employing

13. On the transition from "physicalist" to "de-physicalized" notions of property beginning in the nineteenth century, see MORTON J. HORWITZ, THE TRANSFORMATION OF AMERICAN LAW: THE CRISIS OF LEGAL ORTHODOXY 1870–1960 145–56 (1992).

14. As is explained *infra* text accompanying notes 70–72, those who have examined propertization claims have argued that information asymmetries will lead individuals to trade their rights away and to do so without awareness of what might happen to the information after the first trade is made.

"our" ATM withdrawals, E-ZPass-recorded drives, website visits, and the like for commercial purposes, our perspective easily shifts, and we begin to see "our" data as "our" property. This step is neither logical nor required. It is property protection that makes an asset valuable; value derives from property protection rather than the other way around. It is worth exploring why it is so easy to lose sight of this important fact. To explore this problem and the issue of commodification more generally, I revisit an older case involving potential property rights in human tissue, *Moore v. Regents of California*.[15] Although *Moore* does not deal directly with rights to information, the opinions in *Moore* reveal how even judges holding the same view of the moral stakes in self-commodification can reach diametrically different conclusions about what to do in the face of the changes wrought by technology. The opinions also illustrate the allure of envy-based claims, as it was only after others revealed the value of the patient-plaintiff's tissue that the patient claimed property rights in his excised cells. Several justices would have recognized those claims.[16]

Part III returns to the specific policy problems presented by EHRs and by personal information. A workable EHR policy will take account of a wide variety of values, issues, and interests. Incentives must be created to facilitate EHR adoption, standards must be set to insure interoperability, malpractice rules must be adjusted to accommodate new practices (not to mention new mistakes), and procedures must be developed to enable use of EHR data for public health purposes. With respect to personal information more generally, complex considerations of confidentiality, efficiency, and national security, just to name a few, will all come into play. In the context of both EHRs and personal information more broadly, the multitude of issues presented is likely to be resolved by statutes or regulations that will address in detail the difficult policy questions raised. But because "property" means such different things to different people, it is not clear how much guidance property theory can provide to lawmakers about the appropriate mix or balance of private and public interests in information. Claims for control through propertization of information often rely on a thin Blackstonian "despotic dominion" vision of property that, despite a commonsensical appeal, ignores the many ways in which contemporary property law limits owners' freedom. Just as it is untrue that where there is value there must be property, it is also untrue that where there is property, owners will gain unfettered powers of control. A workable policy for EHRs and for personal information will no doubt provide individuals *some* control rights. These

15. Moore v. Regents of Univ. of Cal., 793 P.2d 479 (Cal. 1990).

16. As is developed *infra* note 215, deceit may also play a role in making property frames more salient. For a particularly affecting account of this phenomenon, see REBECCA SKLOOT, THE IMMORTAL LIFE OF HENRIETTA LACKS (2010), describing a family's reaction to learning that cells taken without consent from a relative had been made into one of the most important and frequently used cell lines in medicine, without a penny of compensation to the patient or any of the members of her family.

rights might look, in the eyes of some, like property rights. But if control rights are granted, it will not be because "property" demands them, but because other considerations of health and public policy do.

All this raises the question of when and whether property might ever provide the control that advocates of information-as-property desire. In a world of de-physicalization and digitization, ownership may not provide the kind of power that old-fashioned property rhetoric invokes. This state of affairs is not necessarily one to be lamented. The question of how power and control over information will be apportioned involves hard choices. But because property theory is itself deeply divided over the extent to which property provides control, "property" itself cannot determine how these choices should be made. "Property" may never have actually given owners as much control as the new adherents of property in information envision. Even if it did, in a world of increasing interconnection, it may be good to be reminded that power and control are themselves always shared.

I. The Need to Control Information

Section A of this Part surveys briefly how EHRs work and how they can improve the quality of health care. There is much to be said about EHRs as a matter of medical, fiscal, and public health policy, but my focus in this section is how the digitization of medical information in EHRs—the very feature that makes EHRs superior to older, paper records—raises security risks quite different from, and more serious than, those posed by paper charts. While HIPAA purports to address these security problems, few believe that HIPAA is adequate to the task. Thus, medical information, like other information collected about users in cyberspace, is insecure, and that insecurity has led to calls for control.

Section B of this Part describes the proposal that property be used to solve the problem of information control. Arguments for property rights in personal information assert that such rights will give individuals a veto power over unwanted uses. As skeptics have observed, however, fully alienable rights may just replicate, and not solve, the security problem, for a variety of forces may conspire to pressure owners to trade their rights away. We could adjust or limit the alienability of such rights to compensate for these forces, but the resulting powers retained by owners might not have the consolidated, *in rem* qualities that, in the eyes of some property theorists, make property distinct. Proposals for propertization of information thus expose fractures in contemporary understandings of how property functions.

Section C of this Part examines whether the venerable "bundle of rights" metaphor for property might or might not fit propertized rights in information. A fully integrated, networked system of EHRs will require lots of customized rights, tweaked between and among various participants in the system. Such customization makes the bundle of rights metaphor seem

apt. At some point, however, under a regime of customization one wonders whether owners will retain robust powers of exclusion or whether their rights will be meaningfully standardized. Since some property theorists consider exclusion and standardization to be core features of property, customization, like alienation, raises the question of how "property" should be defined.

A. *EHRs and Information Control*

The medical record of the past was a paper chart.[17] Such records are difficult to organize and often illegible. The file in one health provider's office is unlikely to be connected in any way to files in other health providers' offices, impeding coordination of care. Frequently, paper records cannot be retrieved in a timely fashion.[18] For these reasons, among others, the medical record of the future will be digital, an electronic health record. Adoption of EHRs has been a priority of prestigious nonpartisan policy organizations such as the Institute of Medicine, as well as of both Republican and Democratic presidential administrations.[19]

There is no single, agreed-upon definition of an EHR,[20] but the components are well understood. An EHR comprises "electronic documentation of

17. Paul M. Schwartz, *Privacy and the Economics of Personal Health Care Information*, 76 TEX. L. REV. 1, 13 (1997) (describing the paper medical record as "a relic from another era").

18. COMM. ON QUALITY OF HEALTH CARE IN AM., INST. MED., CROSSING THE QUALITY CHASM 15 (2001) ("[F]or most individuals . . . health information is dispersed in a collection of paper records that are poorly organized and often illegible, and frequently cannot be retrieved in a timely fashion, making it nearly impossible to manage many forms of chronic illness."); *see also* Lawrence O. Gostin, *Health Information Privacy*, 80 CORNELL L. REV. 451, 457 (1995) (explaining that paper records "are fragmented, poorly documented and duplicative; they are often not accurate, complete, timely, or accessible when needed for patient care").

19. COMM. ON QUALITY OF HEALTH CARE IN AM., *supra* note 18, at 17 (recommending a "national commitment to building an information infrastructure" and to "the elimination of most handwritten clinical data by the end of the decade"). The Bush administration set the goal of making EHRs available to most Americans by 2014. *See* Mike Allen, *Bush Touts Plan for Electronic Medicine: Campaign Aimed at 'Wired' Voters*, WASH. POST, May 28, 2004, at A8; Bernard Wysocki Jr., *Electronic Health Records Get a Push*, WALL ST. J., July 21, 2004, at D4. The Obama administration apportioned twenty-seven billion dollars over ten years to fund EHR development. *See* David Blumenthal & Marilyn Tavenner, *The 'Meaningful Use' Regulation for Electronic Health Records*, 363 NEW ENG. J. MED. 501 (2010); Robert Pear, *New Rules on Electronic Health Records*, N.Y. TIMES, July 14, 2010, at A16; *see also* David Brown, *Obama Pledges New Data System for Veterans*, WASH. POST, Apr. 10, 2009, at A2 (describing EHRs as key feature of Obama's health-care reform plans).

20. Sharona Hoffman & Andy Podgurski, *Finding a Cure: The Case for Regulation and Oversight of Electronic Health Record Systems*, 22 HARV. J.L. & TECH. 104, 108 (2008) ("No universally accepted definitions have been developed for 'EHRs' or 'EHR systems.' ").

There is now one statutory definition, contained in the Health Information Technology for Economic and Clinical Health (HITECH) Act, which was signed into law as a part of the American Recovery and Reinvestment Act of 2009:

providers' notes, electronic viewing of laboratory and radiological results, e-prescribing, and an interoperable connection via a health information exchange with all other providers and hospitals in a community."[21] Interconnection is a non-trivial component of EHRs because of network effects: "The more providers that are connected, the more comprehensive and useful the medical information is for any single patient."[22]

EHRs have the potential to improve the safety, quality, and efficiency of care.[23] With respect to safety, for example, EHR systems have the capacity to reduce prescribing errors by flagging erroneously entered orders, noting drug allergies, and alerting health care providers to potentially problematic drug interactions.[24] With respect to quality, EHRs contain reminder systems for preventative care such as vaccinations or screening; they facilitate management of chronic conditions over time (by tracking past and present laboratory test results) and across providers (by providing information to multiple specialists who can better coordinate care);[25] and they contain decision support features linking providers to information on best practices and

---

> Qualified electronic health record—The term 'qualified electronic health record' means an electronic record of health-related information on an individual that—
>
> (A) includes patient demographic and clinical health information, such as medical history and problem lists; and
>
> (B) has the capacity—
>
> (i) to provide clinical decision support;
>
> (ii) to support physician order entry;
>
> (iii) to capture and query information relevant to health care quality; and
>
> (iv) to exchange electronic health information with, and integrate such information from other sources.

42 U.S.C.A. § 300jj (West 2011); American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, 123 Stat 115 (2009).

21. Cong. Budget Off., Evidence on the Costs and Benefits of Health Information Technology, Pub. No. 2976, at 5 (2008), *available at* http://www.cbo.gov/sites/default/files/cbofiles/ftpdocs/91xx/doc9168/05-20-healthit.pdf. The Health Information Management Systems Society defines an EHR as follows:

> The Electronic Health Record (EHR) is a longitudinal electronic record of patient health information generated by one or more encounters in any care delivery setting. Included in this information are patient demographics, progress notes, problems, medications, vital signs, past medical history, immunizations, laboratory data, and radiology reports.

Electronic Health Record, Health Info. & Mgmt. Sys. Soc'y (2006), http://www.himss.org/ASP/topics_ehr.asp (last visited Feb. 20, 2012).

22. Hall, *supra* note 7, at 638.

23. Blumenthal & Tavenner, *supra* note 19, at 503.

24. Hoffman & Podgurski, *supra* note 20, at 114; Cong. Budget Off., *supra* note 21, at 14.

25. Comm. on Data Standards for Patient Safety, Inst. Med., Letter Report: Key Capabilities of an Electronic Health Record System 2 (2003) [hereinafter Letter Report]; Hoffman & Podgurski, *supra* note 20, at 112.

new treatments.[26] With respect to efficiency, EHRs reduce the number of repetitive and unnecessary tests.[27] This list just scratches the surface of possible advantages.[28] In addition to improvements to the care of individual patients, EHRs can also promote public health by, *inter alia*, enabling the collection of evidence on the efficacy of treatment alternatives and providing a wide array of data to public health officials.[29]

Individuals' medical information is of interest to a large number of entities, from insurance companies to employers to marketing firms seeking to sell medical equipment or drugs.[30] This is true of information about relatively unremarkable conditions, such as hypertension or acne, and certainly no less true about conditions such as HIV, depression, or sexual dysfunction.[31] Of course, some entities might use information about an individual's health status in ways the individual might find beneficial, such as offering programs geared toward helping people to lose weight, stop smoking, or cope with stress. But many entities might use the same information in ways the individual might deem harmful—to deny employment or insurance, or to stigmatize or embarrass.[32]

---

26. Hoffman & Podgurski, *supra* note 20, at 113–16; LETTER REPORT, *supra* note 25, at 8.

27. LETTER REPORT, *supra* note 25, at 5–6.

28. Other advantages of EHRs over paper records include speeding responses to abnormal test results, *id.* at 7; improved communication with patients, *id.* at 9; and enhanced "searchability," *see* Nicolas P. Terry & Leslie P. Francis, *Ensuring the Privacy and Confidentiality of Electronic Health Records*, 2007 U. ILL. L. REV. 681, 683 (2007).

29. *See generally* Rodwin, *supra* note 7 (describing public health uses of the information in EHRs); Marc A. Rodwin, *Patient Data: Property, Privacy & the Public Interest*, 36 AM. J.L. & MED. 586 (2010) (describing similar uses). Ideally, information provided to public health officials would be deidentified. For more on deidentification, see *infra* notes 42–46 and accompanying text.

30. Sharona Hoffman & Andy Podgurski, *In Sickness, Health, and Cyberspace: Protecting the Security of Electronic Private Health Information*, 48 B.C. L. REV. 331, 334–35 (2007) (describing the range of entities that would find health information useful).

31. Gostin, *supra* note 18, at 454 ("Health information is perhaps the most intimate, personal, and sensitive of any information maintained about an individual.").

32. As Lawrence Gostin has explained:

> Unauthorized access to personal information can be motivated by many factors. These include profiting from the sale of data to information brokers or marketing firms; uncovering sensitive information about famous individuals such as a history of mental illness, HIV infection, or a sexually transmitted disease; possessing information that may be helpful in litigation such as malpractice actions; and using the information to make employment or insurance decisions.

Id. at 487; *see also id.* at 490 (unwanted disclosures may result in economic harms such as loss of employment, insurance, or housing; in social or psychological harm; or in stigmatization).

Congress has responded to this possibility in the case of genetic information. The Genetic Information Nondiscrimination Act of 2008 was enacted on May 21, 2008, to "protect Americans against discrimination based on their genetic information when it comes to health insurance and employment." Genetic Information Nondiscrimination Act of 2008, Pub. L. No. 110-233, 122 Stat. 881 (codified as amended in scattered sections of 26, 29, and 42 U.S.C).

Unfortunately, the more thorough, integrated, and networked the EHR, the more information it contains, and the greater the risk to the individual from its unauthorized disclosure.[33] While a paper chart can be secured simply by placing it in a locked room,[34] securing the information in an EHR is not so easy. For one thing, the number of authorized users of an EHR may be very large; many individuals and entities need to be controlled.[35] For another thing, there are powerful commercial reasons for seeking unauthorized access to medical information, and such unauthorized access may not be illegal.[36] In addition, computer networks can be breached or hacked, computers containing personal information can be stolen, and information can be disclosed inadvertently.[37] Within a fully interoperable health information network, "EHRs could be accessed from anywhere in the country and transmitted illicitly across the world quickly, cheaply, and with little risk of detection."[38]

Of course, medical information is subject to duties of confidentiality.[39] However, these duties protect patients only incompletely. Confidentiality attaches to information provided in the course of the physician-patient relationship, but much information in EHRs involves either other health care professionals, who may not be subject to confidentiality duties, or involves other entities, such as insurers or employers, who clearly are not subject to

---

For a discussion of this statute, see Jessica L. Roberts, *The Genetic Information Nondiscrimination Act as an Antidiscrimination Law*, 86 NOTRE DAME L. REV. 597 (2011).

33. Nicolas Terry explains this problem as follows:

> The patient data contained in modern longitudinal systems is comprehensive, portable, and manipulable. The potential for abuse is immense; there are many parties (pharmaceutical companies and government being the obvious examples, inquisitive healthcare employees being the most commonly reported) that crave access to this data. As a result, the privacy and confidentiality costs potentially incurred by patients rise exponentially.

Nicolas P. Terry, *What's Wrong with Health Privacy?*, 5 J. HEALTH & BIOMEDICAL L. 1, 23 (2009).

34. Gostin, *supra* note 18, at 493–94 ("Manual records are often maintained by the health care provider in secure locations . . . . The cumbersome nature of manual records makes it an arduous task to acquire, copy, and use them. . . . By contrast, computerization makes it easy to enter, transmit, copy, or delete vast amounts of data."); Terry & Francis, *supra* note 28, at 705 ("In order to gain access to paper records, someone must be physically present with the record. Inadvertent release of records and computer hacking are notorious problems with other electronic records."). Securing physical records does not guarantee control of the information therein, as doctors might, for example, discuss a patient in a hospital hallway or elevator. On existing legal distinctions between physical patient records and the information contained therein, see *infra* text accompanying notes 90–94.

35. Gostin, *supra* note 18, at 485–86.

36. *Id.* at 487.

37. *See* Hoffman & Podgurski, *supra* note 30, at 332–33; *see also* Kevin Sack, *Patient Data Landed Online After a Series of Missteps*, N.Y. TIMES, Oct. 6, 2011, at A16 (describing inadvertent disclosure of patient information).

38. Hoffman & Podgurski, *supra* note 20, at 121.

39. Gostin, *supra* note 18, at 508.

these duties at common law.[40] Uncertainty about the extent to which disclosures will be protected may deter patients from revealing sensitive information, resulting in the patients receiving sub-optimal care.[41]

The security provisions of HIPAA attempt to respond to this problem. The statute and regulations promulgated under it require that "covered entities" ensure the confidentiality of electronic health information, protect the data against foreseeable threats to security, and safeguard against impermissible use.[42] Yet many commentators believe that HIPAA will not in fact solve the problem of patient confidentiality. A number of complaints have been raised about HIPAA. First, it does not apply to a broad range of actors, from websites to employers, who may possess sensitive health information.[43] Where it does apply, it provides too much discretion to "covered entities" to decide how to implement security standards.[44] Lastly, it fails to provide a private right of action for unauthorized disclosures.[45] As one commentator summarizes the problem, "the privacy architecture seems backwards; it concentrates almost exclusively on the process of patient consent to disclosure."[46]

If HIPAA and its accompanying regulations are indeed flawed, then, despite its nominal confidentiality, medical information is not in fact as secure as most people expect. If this is true, then—again despite its nominal confidentiality—medical information is appropriately conceptualized as but a subset of the personal information collected about individuals in today's networked world. The dystopia of ubiquitous information collection and

---

40. *Id.* at 512; Terry, *supra* note 33, at 18 ("A concept of privacy-confidentiality protection that is bound to an outdated conception of the confidence inherent in a single physician-patient relationship was bound to fail when the physician-patient relationship was replaced by fragmented care."); *see also* Mark A. Rothstein, *The Hippocratic Bargain and Health Information Technology*, 38 J. L. MED. & ETHICS 7, 8 (2010) (asserting that the physician is no longer the "sole provider of health care" but shares responsibility with, inter alia, pharmacists, dentists, and laboratory technicians; "the addition of all these individuals and entities into what was once a simple, two-party, physician-patient relationship has completely changed the original privacy 'bargain' ").

If insurers or employers are "covered entities" under HIPAA, they will be subject to statutory duties to secure patient information. On the limits of HIPAA, see *infra* text accompanying notes 43–46.

41. Hoffman & Podgurski, *supra* note 30, at 335 (describing a survey in which some respondents claimed that to protect their own privacy, they avoided medical tests or physician visits); Rothstein, *supra* note 40, at 9; Schwartz, *supra* note 17, at 22.

42. Hoffman & Podgurski, *supra* note 30, at 339.

43. *Id.* at 344.

44. *Id.* at 350.

45. *Id.* at 354; Terry, *supra* note 33, at 7.

46. Terry, *supra* note 33, at 30; *see also* Peter D. Jacobson, *Medical Records and HIPAA: Is It Too Late to Protect Privacy?*, 86 MINN. L. REV. 1497, 1504–04 (2002) (citing HIPAA's costs, complexity, and internal inconsistencies); Terry & Francis, *supra* note 28, at 715. For purposes of this Article, I assume that the critiques of HIPAA are well-founded.

secret information flows has been described many times.[47] It is now more or less common knowledge that information about each of us has been collected in numerous public and private databases; additional information is obtained by the surreptitious tracking of our every move in cyberspace. On a server somewhere are detailed records of our interests, politics, reading habits, professions, ages, incomes, travel, sexual proclivities—no aspect of our lives is unscrutinized. These records, compiled without our knowledge by entities we do not see or know, are traded, sold, and deployed without our permission. While we may find some uses of this information beneficial, such as when our purchase histories become the basis for recommending books we enjoy,[48] there are many potential uses we rightly fear, such as when recorded (but not always verified)[49] indiscretions become the basis for a denying jobs, credit, or insurance.[50] More generally, the massive collection of personal information "creates a potential for suppressing a capacity for free choice: the more that is known about an individual, the easier it is to force his obedience."[51] The specter of constant scrutiny may discourage individuals from testing new behaviors, ideas, or associations.[52] Just as concern about potential later disclosures may deter patients from confiding in their doctors, concern about misuse or misperception of personal information may stifle independent thinking and the experimentation necessary for self-development.[53]

As with HIPAA in the context of medical information, there are federal statutes addressing some of these problems.[54] But, as is the case with

47. In addition to the sources cited *supra* note 5, see Schwartz, *supra* note 17, at 1621–32 (describing "The Privacy Horror Show").

48. SOLOVE, *supra* note 5, at 23.

49. *Id.* at 21.

50. *Id.* at 2; Schwartz, *supra* note 17, at 22–33.

51. Paul M. Schwartz, *Privacy and Participation: Personal Information and Public Sector Regulation in the United States*, 80 IOWA L. REV. 553, 560 (1995).

52. Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609, 1656–57 (describing the phenomenon of "cyber-Thought Police" and arguing that if Internet users "gain a sense that their every mouse click and key stroke might be observed, the necessary insulation for individual self-determination will vanish").

53. *See, e.g.*, Jack M. Balkin, *Information Power: The Information Society from an Antihumanist Perspective* 9, *in* THE GLOBAL FLOW OF INFORMATION 232 (Eddan Katz & Ramesh Subramanian eds., 2011) ("Increasingly, software architectures and information networks direct, block, filter, categorize, monitor and normalize behavior: they drive the pace and possibilities of human interaction, the scope of human imagination, and the search for and realization of human desires."). For more on self-development, see *infra* text accompanying notes 141–145.

54. For a listing of federal statutes passed since 1970, see DANIEL J. SOLOVE & PAUL M. SCHWARTZ, INFORMATION PRIVACY LAW, 36–38 (2d ed. 2009). Examples include Children's Online Privacy Protection Act of 1998, Pub. L. No. 106-170, 15 U.S.C. §§ 6501–6506 (records from children under age 13 gathered by Internet websites); Fair and Accurate Credit Transactions Act of 2003, Pub. L. No. 108-159, 15 U.S.C. § 1681 and 20 U.S.C. §§ 9701-9708 (amends Fair Credit Reporting Act and provides additional protections against identity theft); Video Privacy Protection Act of 1988, Pub. L. No. 100-618, 18 U.S.C. §§ 2710–2711

HIPAA, most commentators regard these statutes as inadequate in a multitude of ways. They reach only a fraction of the information collected about us—our video rental records, for example—and only a fraction of the collectors of that information.[55] Common law causes of action by no means fill these gaps.[56]

If, like HIPAA, the patchwork of federal and state laws pertaining to information is indeed but a patchwork, then there is little to retard the flow of personal information. The law does not ensure that individuals will control the personal data collected about them.[57] Since out-of-control information can be so dangerous, it seems logical to search for a legal device that will provide individuals with at least some of the desired control. Property is one possibility; if individuals are deemed to own their personal information, then they can decide for themselves how that information will be used.[58] It is to these arguments about property that I now turn.[59]

(videotape rental information); Family Educational Rights and Privacy Act of 1974, Pub. L. No. 93-380, 20 U.S.C. §§ 1221 note, 1232g (school records); Cable Communications Policy Act of 1984, Pub. L. No. 98-549, 47 U.S.C. § 551 (records maintained by cable companies).

55. *See* Daniel J. Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy*, 53 STAN. L. REV. 1393, 1444 (2001) ("[F]ederal statutes cover only a small geography of the database problem. They form a complicated patchwork of regulation with significant gaps and omissions. For example, federal regulation. . . does not cover most records maintained by state and local officials, as well as a host of other records held by libraries, charities, and merchants (i.e., supermarkets, department stores, mail order catalogs, bookstores, and the like)."); *see also* SOLOVE & SCHWARTZ, *supra* note 54, at 37–38 (listing federal statutes mandating the collection of sensitive personal information in contrast to the statutes protecting that information).

56. Joy L. Pritts, *Altered States: State Health Privacy Laws and the Impact of the Federal Health Privacy Rule*, 2 YALE J. HEALTH POL'Y, L. & ETHICS 325, 331 (2002) (explaining that inability of plaintiffs to meet "highly offensive" standard for invasion of privacy based on unreasonable public disclosure of private facts often leaves them no remedy for harm); Neil M. Richards & Daniel J. Solove, *Prosser's Privacy Law: A Mixed Legacy*, 98 CAL. L. REV. 1887, 1923 (2010) (arguing that privacy torts are insufficient to address modern privacy problems because rigid causes of action force harm to fit standards not tailored to modern privacy needs); *see also* Schwartz, *supra* note 52, at 1632 ("Legal protection of personal information on the Internet is generally limited and often incoherent.").

57. *See, e.g.*, Cohen, *supra* note 6, at 1379 ("Data privacy advocates seek . . . to guarantee individuals control over their personal data."); Julie E. Cohen, *Cyberspace As/And Space*, 107 COLUM. L. REV. 210, 245 (2007) ("Control of [data] flows has assumed paramount importance in the interlinked realms of intellectual property and privacy."); Kang, *supra* note 5, at 1205 ("[I]nformation privacy is 'an individual's claim to control the terms under which personal information . . . is acquired, disclosed, and used.' "); Schwartz, *supra* note 52, at 1659 ("From the age of computer mainframes in the 1960s to the current reign of the Internet's decentralized networks, academics and the law have gravitated towards the idea of privacy as a personal right to control the use of one's data.").

58. Samuelson, *supra* note 8, at 771–72 (suggesting that "propertizing personal information" simply extends the large, existing market for information in personal data in a way that grants individuals control, but noting also that commodification of personal data may offend those "who embrace a civil rights concept of data privacy").

59. As noted earlier, property is obviously not the only legal category that could apply. *See supra* note 9. One obvious alternative is "intellectual property," the (largely) statutory system of patent, copyright and trademark. But, as is developed later, the "fit" between IP and

B. *Can Property Solve the Problem of Information Control?*

The simplest argument for property rights in personal information is based on Calabresi and Melamed's famous distinction between property and liability rules.[60] In this scheme, property rules give individuals veto rights over the use of assets, while liability rules permit unconsented-to uses of those assets, requiring only payment of damages for any loss suffered as a result of that use. Or, as Lawrence Lessig has explained in arguing for property rights in personal information, "a property regime requires negotiation before taking; a liability regime allows a taking, and payment later."[61] Because a property rule would bar use of personal information without prior negotiation, it provides exactly the sort of control that has been sought to counteract the dystopia of ubiquitous-but-secret information flows. Lessig justifies the call to property rights in exactly these terms: "The key to a property regime is to give control, and power, to the person holding the property right."[62]

In a world of propertized information, it will be up to each individual to decide for himself or herself whether—and at what price—to trade his or her personal information.[63] Granting individuals property rights in their per-

---

information assets is messy. *See infra* note 66. In any event, the Supreme Court has held that raw data—facts—are not protected by intellectual property law. Feist Publ'ns, Inc. v. Rural Tel. Serv. Co., 499 U.S. 340 (1991).

Another legal category that might appear to provide a means of controlling information is "privacy." As a legal category, however, privacy is a pretty slippery fish. Privacy's core principles and their reach are much disputed. *See* DANIEL J. SOLOVE, UNDERSTANDING PRIVACY 1 (2008) (describing privacy as "a concept in disarray"). I take no position on these disputes here. I note only that, with respect to personal information, many scholars conceptualize privacy as the problem, not the solution. *See, e.g.*, Kang, *supra* note 5, at 1201, 1267–73 (proposing a "Cyberspace Privacy Act").

Contract and tort are other obvious possibilities. Contract principles would, of course, be parasitic on property; one can only bargain with what one owns. On contract, see Kang, *supra* note 5, at 1246–48 (exploring the possibility that individuals could bargain for the level of data secrecy they desire, but noting that "for numerous reasons, such as transaction costs, individuals and information collectors do not generally negotiate and conclude express privacy contracts before engaging in each and every cyberspace transaction"). On tort, see Litman, *supra* note 6, at 1308–09 (suggesting that uses of information to which individuals have not consented can plausibly be seen as breaches of trust, but acknowledging that this theory requires an extension of existing doctrine to cover entities not usually considered to owe duties of confidentiality to individuals). I leave to others with greater expertise the task of examining whether and how contract or tort solutions might work.

60. Guido Calabresi & A. Douglas Melamed, *Property Rules, Liability Rules, and Inalienability: One View of the Cathedral*, 85 HARV. L. REV. 1089 (1972).

61. LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE 160 (1999). For an argument that Lessig misapplies the Calabresi/Melamed framework, see Paul M. Schwartz, *Beyond Lessig's* Code *for Internet Privacy: Cyberspace Filters, Privacy Control, and Fair Information Practices*, 2000 WIS. L. REV. 743, 77–76.

62. LESSIG, *supra* note 61, at 160.

63. *Id.* at 161; *see also* Kenneth C. Laudon, *Markets and Privacy*, 36 COMM. OF THE ACM 92, 93 (1996) ("[T]o ensure the protection of individual privacy beyond 2000 we should

sonal information might allow them, it is argued, to "capture some of the value their data have in the marketplace."[64] The need to account for those rights might affect the behavior of the firms that currently collect data: "perhaps firms would collect or process less personal data than they currently do if they had to pay individuals for rights to do so."[65] The propertization argument asserts, in other words, that giving individuals property rights in their personal information may result in less unwanted, secret collection of such information.

Since personal information is not protected by existing intellectual property law,[66] if personal information is to be protected as property, it will be protected as ordinary property, under ordinary, not intellectual, property principles. But at least some ordinary property principles could be problematic in the case of personal information. One that is seen as particularly troublesome is the principle of free alienability. As a general rule, applicable in ordinary circumstances, property is indeed freely alienable, and the law is hostile to many alienation restraints.[67] Property's alienability is thought to be socially beneficial because it enables welfare-enhancing trades that move assets to the users who value them most highly.[68] But many commentators predict that the free trade in personal information enabled by propertization will lead to lesser, rather than greater, control by the individuals to whom the information pertains.[69] If individuals have property rights to personal information, those individuals will determine as an initial matter whether to sell that information for money or barter it for services such as access to a website.[70] But they will not be able to determine the use made of that information once it is in the hands of another; after the individual trades the

consider market-based mechanisms based on individual ownership of personal information and a National Information Market.").

64. Samuelson, *supra* note 7, at 1129.

65. *Id.* at 1133.

66. The personal information of concern here does not quite fit any of the existing IP categories, as it involves no invention or innovation that would make it patentable, it lacks the originality and creativity that would make it eligible for copyright protection, and it is not the sort of secret business information that would make it a trade secret. IP scholars have argued, in addition, that the incentives that the IP system provides are unnecessary. As one commentator explains, "Intellectual products have strong public good characteristics, and (at least in theory) would be underproduced without the additional incentives that intellectual property provides." Cohen, *supra* note 6, at 1387; *see also* J.H. Reichman & Pamela Samuelson, *Intellectual Property Rights in Data?*, 50 VAND. L. REV. 49, 165 (1997) (arguing that classical IP laws are meant to stimulate forms of creative endeavor that would not be developed without the institution of exclusive property rights). However, "incentives play little role in the analysis [of personally-identified data]; personally-identified data is not scarce." Cohen, *supra* note 6, at 1387. For similar arguments, see Mark A. Lemley, *Private Property*, 52 STAN. L. REV. 1545, 1550 (2000); Samuelson, *supra* note 7, at 1139–41.

67. JOSEPH WILLIAM SINGER, PROPERTY 278–80 (3d ed. 2010)

68. *Id.* at 279.

69. *See, e.g.*, Cohen, *supra* note 6, at 1391 ("Recognizing property rights in personally-identified data risks enabling more, not less, trade and producing less, not more, privacy.").

70. Litman, *supra* note 6, at 1299–30.

information away, it is freely alienable by the buyer for uses of which the individual seller may disapprove.[71] This problem is enhanced by information asymmetries between information sellers and information buyers; individuals rarely understand the kind and range of uses that might later be made of the information they are selling.[72] In the context of personal information, alienability, ordinarily thought to be welfare-enhancing, becomes something more like a trap for the unwary.

Of course, many of these arguments against propertization assume that if something is "property," then it must be fully and completely alienable.[73] This assumption is, it has been noted, somewhat simplistic.[74] Many valuable assets that are commonly regarded as property are not, in fact, fully alienable—social security and pension benefits are easy examples.[75] Moreover, "alienability is not a binary switch to be turned on or off, but rather a dimension of property ownership that can be adjusted in many different ways."[76] Thus, Paul Schwartz has offered what he describes as a "hybrid alienability" model of property rights in personal information,[77] one which would "permit the *transfer* for an initial category of *use* in personal data, but only if the customer is granted an opportunity to block further transfer or use by unaffiliated entities."[78] Similarly, Julie Cohen has suggested the possibility of a property right in personal information that might look more like the limited ownership rights granted under copyright law than a "traditional 'property'

71. *Id.* at 1300; Samuelson, *supra* note 7, at 1138; *see also* Cohen, *supra* note 6, at 1391 ("Thus far, whether deliberately or by oversight, we have constructed data processing systems that do not involve the individual in decisionmaking about the uses of data collected by the system."); Schwartz, *supra* note 7, at 2097 (arguing that information asymmetries about data collection and processing and the difficulty of providing understandable privacy notices are problems for a "data trade model under which consumers have only a single chance to negotiate future uses of their information").

72. Schwartz, *supra* note 7, at 2078 ("[C]onsumer ignorance leads to a data market in which one set of parties does not even know that 'negotiating' is taking place. Even if there is a sense that some personal data are collected, many individuals do not know how or whether this information is further processed or shared."); *see also* Cohen, *supra* note 6, at 1397 (stating that individuals "face enormous difficulty assessing how their personal information will be used" and lack information about secondary and tertiary uses of personally identified information).

73. *See, e.g.*, Litman, *supra* note 6, at 1299 ("[I]f a right is proprietary, it is normally fully alienable.").

74. Schwartz, *supra* note 7, at 2093 ("[T]he idea that free alienability is an inexorable aspect of information-property is . . . a problematic cartoon."); *see also* Cohen, *supra* note 6, at 1382–84 (describing alternatives to "the dominant liberal market-based understanding of property").

75. On inalienability generally, see Susan Rose-Ackerman, *Inalienability and the Theory of Property Rights*, 85 COLUM. L. REV. 931 (1985).

76. Lee Anne Fennell, *Adjusting Alienability*, 122 HARV. L. REV. 1403, 1408 (2009).

77. Schwartz, *supra* note 7, at 2094.

78. *Id.* at 2098. Schwartz's model also includes an "opt-in default" under which "any further use or transfer would require the customer to opt in—that is, it would be prohibited unless the customer affirmatively agrees to it." *Id.*

right—a right against all comers and all uses."[79] These proposals may or may not carry the day, but they demonstrate that it may be possible to construct a right in personal information that could plausibly be characterized as a "property" right, but that is not fully alienable.

The rights individuals would have under these proposals are a good deal more complex, and a lot less clear, than traditional property rights in tangible goods. An individual's rights against one entity—say, the first transferee of the individual's information—might not be the same as that individual's rights against other entities, such as subsequent transferees. Property rights in medical information would almost certainly have this quality, with an individual being able to assert some rights against, say, her physician, and different rights against, say, her insurer.

Whether the complicated set of rights contemplated here is appropriately characterized as "property" depends, of course, on how "property" is defined. If one understands property to accord a single, identifiable owner a set of consolidated rights that grant nearly absolute control,[80] the rights granted to individuals under these tailored control regimes might not qualify as "property" rights at all. Many people or entities (patients, physicians, insurers, employers) will simultaneously have ownership rights in the information contained in EHRs, with no single individual having anything like absolute control.

Similarly, if one understands property as a set of rights *in rem*, good against all the world,[81] it would be hard to see the rights granted under these complex regimes as "property" rights. *In rem* rights "have an impersonality and generality that is absent from rights and privileges that attach to persons directly."[82] They send simple signals that avoid the need for decision makers to inquire what uses an owner is making of her property or the identity of those who owe duties to the owner.[83] They operate largely within a regime of standardization that prevents recognition of information-inefficient, specialized forms.[84] But in the complicated ownership regimes offered for

79. Cohen, *supra* note 6, at 1428–29.

80. *See* Joseph William Singer, *No Right to Exclude: Public Accommodations and Private Property*, 90 NW. U. L. REV. 1283, 1453 (1996) (describing the "classical conception" of property); *see also* LAURA UNDERKUFFLER, THE IDEA OF PROPERTY 39 (2003) (describing a "common" conception of property); Joan Williams, *The Rhetoric of Property*, 83 IOWA L. REV. 277, 280–83 (1998) (describing the "intuitive image of absoluteness").

81. On property as an *in rem* right, see, for example, Thomas W. Merrill & Henry E. Smith, *The Property/Contract Interface*, 101 COLUM. L. REV. 773, 777 (2001); Henry E. Smith, *Self-Help and the Nature of Property*, 1 J.L. ECON. & POL'Y 69, 79 (2005).

82. Thomas W. Merrill & Henry E. Smith, *What Happened to Property in Law and Economics?*, 111 YALE L.J. 357, 359 (2001).

83. Henry E. Smith, *Exclusion and Property Rules in the Law of Nuisance*, 90 VA. L. REV. 965, 978 (2004).

84. *See generally* Thomas W. Merrill & Henry E. Smith, *Optimal Standardization in the Law of Property: The* Numerus Clausus *Principle*, 110 YALE L.J. 1 (2000) (explaining why property rights, unlike contract rights, are restricted to a limited number of standardized forms).

propertized information, not all—and maybe not any—rights will be good against all the world. And the whole idea of customizing alienability in a propertized information regime is inconsistent with the standardization that information-based theories of property hold to be essential.

Neither of these two understandings of property—as consolidated rights, or as rights *in rem*—is uncontroversial.[85] But that is my point. The proposals to use the legal category "property" as a means to control unseen flows of personal information raise questions of what property is and does as a legal category. It may be that we can create a novel legal regime tailored and customized to deal with the problems particular to information. But at some point, the departure of that regime from existing models of property might raise the question of whether the regime deserves the name "property" at all. It depends, of course, on what property is.

C. *Bundles of Rights in Information*

Tailored, customized rights in information fit more comfortably with a vision of property as a bundle of rights. While the bundle-of-rights metaphor has always had its critics,[86] and while the metaphor has been under particularly heavy weather recently,[87] there are some aspects of the bundle of rights conceptualization that are not particularly controversial. It is widely agreed upon that owners have multiple rights with respect to what they own—they can use it, exclude others, sell it, give it away, and so forth.[88] There is little doubt also that property rights in a single asset can be divided among people (as where one person owns surface rights and another rights to the subsurface) and divided over time (as where one person holds a life estate and another a remainder).[89] Ownership rights in EHRs correspond fairly easily to this picture. Patients' ownership of their medical information might accord them multiple rights—say, to inspect their records, or to control who

85. Indeed, both have been subject to sustained criticism. On consolidation, see Singer, *supra* note 80, at 1453, 1459–60. On *in rem*, exclusion-based, theories, see, for example, Gregory S. Alexander, *The Complex Core of Property*, 94 Cornell L. Rev. 1063 (2009). For a summary of the disputes within contemporary property theory about property's social function, see Jane B. Baron, *The Contested Commitments of Property*, 61 Hastings L.J. 917 (2010).

86. *See, e.g.*, J.E. Penner, *The "Bundle of Rights" Picture of Property*, 43 UCLA L. Rev. 711 (1996).

87. Merrill & Smith, *supra* note 81, at 787; Merrill & Smith, *supra* note 82, at 360; Henry E. Smith, *Property as the Law of Things*, 125 Harv. L. Rev. (forthcoming 2012) (manuscript at 10, 14), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2012815. For an overview and analysis of contemporary debates about the bundle-of-rights metaphor, see Baron, *supra* note 85, at 933–53.

88. Joseph William Singer, Property Law: Rules, Policies, and Practices 607 (5th ed. 2010) ("An owner of a fee simple interest in real property has the present right to possess and use the property, the right to sell it or give it away, and the right to devise it by will or leave it to her heirs.").

89. *Id.* at 595 (describing divisions of ownership over time).

sees them. And multiple people or entities—the patient, the doctor, the laboratory, the insurance company—might have different, divided ownership interests in the information in the EHR.

Even before digitization, rights in medical information were broken into discrete pieces that seemed to render the bundle-of-rights concept particularly apt. Some case law and some statutes[90] held that physicians or hospitals owned the physical charts in which patient information was recorded, while patients owned—or had a right of access to—the information contained in those charts.[91] Other courts described the doctor's right to treatment records as "custodial," and the patient's right of reasonable access to those records as "a 'property' right."[92] Still other courts held that doctors had a "primary right to possess" medical records, with the patient having access rights.[93] A recent article in the Journal of the American Medical Association explains the "rudimentary points" of medical record ownership as follows:

> Clinicians, as owners of the paper records they maintain, can give or sell medical records to other clinicians for treatment purposes and block access by anyone except the patient. Patients have rights of privacy and access to their records, but neither federal nor state law explicitly extends property rights to patients. For instance, patients do not have the right to sole possession or to the destruction of their original records.[94]

---

90. *See* LA. REV. STAT. ANN. § 40:1299.96 (2011) (stating that medical records are the property of the health care provider, but patients have a right of access); MISS. CODE ANN. § 41-9-65 (West 2011) (stating that medical records are the property of the hospital, with the patient having a right to access contingent on showing "good cause"); VA. CODE. ANN. § 54.1-2403.3 (2011) (stating that medical records are the property of the health care provider maintaining them, with an exception for information disclosure to the patient); *see also* N.H. REV. STAT. ANN. § 332-I:1 (West 2011) ("[A]ll medical information contained in the medical records in the possession of any health care provider shall be deemed to be the property of the patient.").

91. *See, e.g.*, Wallace v. Univ. Hosp. of Cleveland, 82 Ohio Law Abs. 257 (1959) ("[I]t is true that the original Hospital records are the property of the Hospital. . . . [H]owever, it is also true that the patient has a property right in the information contained in the record and thus is entitled to a copy of it.").

92. *In re* Striegel, 399 N.Y.S.2d 584, 585–86 (1977); *see also* MICH. COMP. LAWS ANN. § 333.26265 (West 2011) (stating that patient has the right to examine or obtain his medical record); S.C. CODE ANN. § 44-115-30 (2011) (explaining the right to receive a copy of record and transfer record to another physician).

93. Cornelio v. Stamford Hosp., No. CV 960155779S, 1997 WL 430619, at *7 (Conn. Super. July 21, 1997); *see also* MO. REV. STAT. § 191.227 (2011) (stating that the right shall be limited to access consistent with the patient's condition and sound therapeutic treatment as determined by the provider); TEX. OCC. CODE ANN. § 159.006 (West 2011) (stating that patient has access to record or summary of record unless physician deems access harmful to the patient).

94. Mark A. Hall & Kevin A. Schulman, *Ownership of Medical Information*, 301 J. AM. MED. ASS'N 1282, 1282 (2009).

This disaggregation of rights—into property (or custody or possession) as opposed to access; into powers of sale or donation as opposed to possession or destruction—invites us to envision property rights as isolated "sticks" that are held by different parties. The bundle-of-rights metaphor suits this picture in that it operates "as a device for separating the various facets of property and for giving an intuitive grasp of their separateness and moveability rather than their interrelatedness and porosity."[95]

Property rights in EHRs are likely to be even more disaggregated and fragmented than those in paper records because digitization increases the number of possible contributors to a patient's record. An integrated EHR might have entries from the patient's primary care physician, multiple specialists, a laboratory, a testing facility, an insurance company, and so on. Thus, there will be more potential claimants to the information in the EHR—more potential "owners," in effect, than just the two (doctor and patient) involved in paper charts. The patient might also have a different right or set of rights with respect to each potential claimant. For example (and wholly hypothetically), a patient might have the power to control precisely what information about, say, an initial diagnosis is distributed to a specialist or employer, but not the same power of control with respect to an insurer. The other contributors to the chart might similarly have non-uniform rights with respect to one another.[96]

To the extent that EHRs involve multiple owners of the same information, with the various owners having a variety of different rights and powers with respect to each other and to the patient, envisioning "property" in medical information in terms of a bundle of rights seems thoroughly appropriate. But here again, as with proposals to limit the alienability of property rights in personal information,[97] the complicated "bundles of rights" that might emerge in EHRs may not, in the eyes of some, function as "property" at all. Again, it all depends on how one defines property and how one understands property to work.

For some, exclusion lies at property's core. Consider, in this regard, one contemporary theorist's account of the way in which property operates:

---

95. Carol M. Rose, Property and Persuasion: Essays On The History, Theory, And Rhetoric Of Ownership 282 (1994).

96. On the limits of various players' control rights in medical information:

> [A]n individual cannot have complete control over her medical information because access to these data is essential for the modern provision of health care. In a similar fashion, physicians must be limited in their ability to negotiate with patients for privacy because of the significant need for personal health care information on the part of insurers, hospitals, and government. A physician and a patient . . . cannot engage in fully customized negotiations because such bargaining might lead to excessive limits on the access to data of such parties as insurance programs. . . . public health agencies, and law enforcement agencies.

Schwartz, *supra* note 17, at 53.

97. *See supra* text accompanying notes 77–79.

> Property gives the right to exclude from a "thing," enforceable against everyone else—it is an in rem right—and a crude delegation to the owner avoids the costs of delineating use rights. On the dutyholder side, the message is a simple one—to "keep out"—and this simultaneously protects a reservoir of uses for the owner without officials and dutyholders needing to know what those might be.[98]

Exclusion is relatively economical: "very rough signals or informational variables—such as presence inside or outside the boundary line around a parcel of land—are employed to protect an indefinite class of uses with minimal precision."[99] On this view, property relies on *in rem* exclusion as a means both to protect owners' use rights and to communicate simply to non-owners their duty to respect those rights.[100]

The bundles of rights in medical records hardly function this way. No single "owner" of the many interests in information in EHRs will have *in rem*-type exclusion rights, nor will there be simple signals that tell either co-owners or non-owners which persons or entities have what rights, powers, or duties. Instead, the complicated, potentially overlapping rights to the information in EHRs will be operationalized by a strategy at the other end of the spectrum from exclusion: the strategy of "governance." Governance rules evaluate interests "on something close to a use-by-use basis; rights are delineated using signals . . . that pick out and protect individual uses and user behavior."[101] The advantage of governance rules "is that they allow society to control resources in non-standard ways that entail greater precision or complexity in delineating use rights than is possible using exclusion."[102] The relative precision of governance rules make them expensive, however, because each legal relation among diverse claimants must be individually

98. Smith, *supra* note 83, at 978; *see also* Henry E. Smith, *Property and Property Rules*, 79 N.Y.U. L. REV. 1719, 1756 (2004) ("[T]he exclusion strategy bunches together a lot of uses and does not inquire into details; it lacks the benefits of precision in terms of maximizing the value of individual uses, say from specialization by different actors in different uses of the same asset. At the same time, the exclusion strategy avoids the costs of precision.").

In recent work, Smith has reiterated that exclusion lies at the "core" or property's "architecture." Smith, *supra* note 87, manuscript at 9. However, Smith goes on to assert that exclusion is not property's core value "because it is *not a value at all*" but rather a means to the end of serving owners' interest in the use of things. *Id.*

99. Smith, *supra* note 83, at 978–79.

100. Smith, *supra* note 81, at 78; Smith, *Property and Property Rules*, *supra* note 98, at 1754.

101. *Id.* at 979; *see also* Merrill & Smith, *supra* note 81, at 791 ("[G]overnance rules typically specify particular uses in some detail, including the identity of the rightholder and the dutyholder. Indeed, often the dutyholder will need to know the identity of the rightholder in order to avoid violating the duty.").

102. Merrill & Smith, *supra* note 81, at 797.

spelled out.[103] Thus, as the number of people who interact with an asset increases, the costs of governance also increase.[104]

Of course, even those who favor the exclusion strategy envision a role for governance where "high stakes" are involved,[105] and where a more precise, user-by-user delineation of entitlements is required.[106] Yet if property's distinct ability to solve social ordering problems derives from its use of relatively crude, simple, inexpensive signals, then the intricately bundled, customized rights to the information in EHRs do not seem to take much advantage of property's unique ability to decide questions "up front and across the board."[107] In this view, the bundled rights in EHRs effectively treat property "as a branch of contract or tort, with no special character as a right to a thing that is good against the world."[108]

In addition to the lack of fit between the exclusion-centered conception of property and the user-by-user delineation of rights to information in EHRs, the highly-customized rights in EHRs are inconsistent with the influential view that rights in property traditionally come—and should come—in a limited variety of standardized forms.[109] This principle, known as *numerus clausus* ("the number is closed"),[110] is, like exclusion, defended on the grounds of information costs.[111] Unusual property rights increase the costs borne by third parties to understand the scope or nature of those rights, but "those creating . . . idiosyncratic property rights cannot always be expected to take these increases in measurement costs fully into account, making them a true externality. Standardization of property rights reduces these measurement costs."[112]

It is theoretically possible that the rights to information bundled in EHRs will take the standardized forms of traditional estates in land. But it seems more likely that the bundles will not be standardized in this way. Indeed, if the rights in EHRs are not customized in fairly elaborate ways, EHRs will be dysfunctional; if each participant's powers and duties are not carefully and deliberately defined, the individual, social, and network bene-

103. Smith, *supra* note 83, at 981.

104. At some point, "the information costs of specifying which individuals have the right to do what will simply become too great." Merrill & Smith, *supra* note 81, at 798.

105. Henry E. Smith, *Institutions and Indirectness in Intellectual Property*, 157 U. PA. L. REV. 2083, 2086 (2009); *see also* Smith, *supra* note 83, at 1024–25 (arguing that where to draw the line between exclusion and governance is an "empirical question").

106. Smith, *supra* note 83, at 975–76; Smith, *Property and Property Rules*, *supra* note 98, at 1797.

107. Henry E. Smith, *Mind the Gap: The Indirect Relation Between Ends and Means in American Property Law*, 94 CORNELL L. REV. 959, 963 (2009).

108. *Id.*; *see also* Merrill & Smith, *supra* note 81, at 787 ("The duty to respect the property of others . . . has an impersonality and generality that is qualitatively different from duties that derive from specific promises or relationships.").

109. Merrill & Smith, *supra* note 84, at 8.

110. *Id.* at 4.

111. *Id.* at 8.

112. *Id.*

fits of EHRs will not be achieved.[113] Thus, the interests in EHRs must be freely customizable, and not standardized. This deprives them of the information cost benefits that some scholars believe make the legal category "property" exceptional.[114]

Just as not all scholars concur that alienability is a defining attribute of property, not all scholars concur that information costs should drive our understanding of what property is and does. There is substantial resistance to the notion that exclusion lies at property's core.[115] For those who believe property should promote human flourishing,[116] freedom,[117] or democracy[118]—just to state a few of the many values property law might serve[119]—the question to be asked about property rights in EHRs is not whether they are framed in terms of exclusion but rather whether they lead to outcomes that can be justified in substantive terms.[120] For these scholars, it is immaterial whether the exclusion or governance strategy governs property rights in EHRs. What matters is the values ultimately served by whatever package of rights is put together.[121]

Similarly, not all scholars agree that standardization is an essential, or even valuable, attribute of property rights. The standard forms of the old estates system, such scholars argue, are only a small portion of today's property system, which has been supplemented by statutes and regulations reaching into wide swathes of social life—from zoning to housing to marriage.[122] Thus, just as we might conceivably customize the alienability of

113. *See supra* text accompanying notes 21–29.

114. Merrill & Smith, *supra* note 82, at 387 (describing the "intolerable" information costs imposed by freely customized rights.); *see also* Merrill & Smith, *supra* note 84, at 27 (describing the high information costs imposed by "fancies," i.e., idiosyncratically created property rights).

115. *See, e.g.*, Alexander, *supra* note 85, at 1066 ("[T]he core [of property] is more complex than exclusion alone."); Hanoch Dagan, Exclusion and Inclusion in Property 8 (June 7, 2009) (unpublished working paper), *available at* http://ssrn.com/abstract=1416580 ("[E]xclusion . . . can exhaust the meaning of property and thus be properly described at its core only if we set aside, somewhat arbitrarily, large parts of what constitutes property law.").

116. *See* Gregory S. Alexander, *The Social-Obligation Norm in American Property Law*, 94 CORNELL L. REV. 745, 745 (2009).

117. *See* Jedediah Purdy, *A Freedom-Promoting Approach to Property: A Renewed Tradition for Old Debates*, 72 U. CHI. L. REV. 1237, 1242 (2005).

118. *See generally* Joseph William Singer, *Democratic Estates: Property Law in a Free and Democratic Society*, 94 CORNELL L. REV. 1009 (2009).

119. On the diversity of values property protects, see Nestor M. Davidson, *Standardization and Pluralism in Property Law*, 61 VAND. L. REV. 1597 (2008).

120. *See, e.g.*, Singer, *supra* note 118, at 1059 ("In defining rights and obligations with respect to property, we are obligated to consider the full range of human values we care about rather than merely thinking quantitatively about how to maximize preferences."); *see also* Baron, *supra* note 85, at 932 (describing how, for progressive property theorists, "what is most interesting and important about property is the outcomes it produces").

121. Baron, *supra* note 85, at 952–53 (describing property theories that "require constant questioning of whether property rules actually serve the values for which they were adopted").

122. Singer, *supra* note 118, at 1052 ("We use a combination of common law, statutes, and social custom to define the boundaries of allowable packages of property rights . . . .").

property rights in EHRs, we might customize to a high degree of precision and complexity the nature and scope of the various participants' rights.

Again, the point here is not that exclusion-centered rights to the information in EHRs would be better (or worse) than bundled governance rights, or that standardizing the bundles would be better (or worse) than tailoring them. The point is that whether any particular configuration of rights to information is appropriately categorized in terms of "property" exposes fault lines in our understanding of what property is and does. Property is a contested concept,[123] and debates over whether property is a useful legal frame in which to organize various participants' interests in the information in EHRs only exposes the lack of agreement about what property is. It is hard to see how the problem of information control can be "fixed" by resort to a legal regime whose substance and scope are pervasively disputed.

II. Information And Property Rhetoric

Section A of this Part begins by reconsidering the harm caused by loss of control of personal information, arguing that at least one component of harm involves an individual's loss of power to determine which facts relating to his or her self are disclosed and how those facts are presented. Because there is no single, agreed-upon definition of the "self,"[124] I consider several possible visions, based on dignity, autonomy, self-determination, and community. Under any of these conceptualizations, definition by others is properly understood as an assault on the self. In the face of such an assault, attempts to (re)gain control of information about oneself through property make good sense. They may be understood as yet another way that property may be used for personhood, as Margaret Radin famously suggested long ago.[125]

Section B focuses on one danger of propertization. As noted earlier, it may be feasible to create tailored, highly customized bundles of rights that address some of the unique aspects of information generally and medical information specifically. Whether or not these bundles solve the practical problem of controlling information, the very notion of property in personal information—in the "self"—creates rhetorical issues. If how we speak about the world matters—and some believe that it matters very much[126]—then we

123. Baron, *supra* note 85, at 918–21.

124. For particularly influential views, see Erving Goffman, The Presentation of Self in Everyday Life (1959); George H. Mead, Mind, Self, and Society (Charles W. Morris, ed., 1934); Charles Taylor, Sources of the Self: The Making of the Modern Identity (1989).

125. Margaret Jane Radin, *Property and Personhood*, 34 Stan. L. Rev. 957 (1982).

126. *See, e.g.*, Margaret Jane Radin, *Market-Inalienability*, 100 Harv. L. Rev. 1849, 1870 (1987) ("Rhetoric is not just shaped by, but shapes, reality."); Carol M. Rose, *Crystals and Mud in Property Law*, 40 Stan. L. Rev. 577, 604–10 (discussing the importance of our choice of rhetoric and metaphor).

ought to consider whether talking about our "selves" as commodities is or is not a good thing. We ought to consider, also, whether in our current non-ideal world, where information is already bought and sold like ordinary property in the hands of, *inter alia*, database aggregators, we can avoid a property frame.

Section C takes up the casebook chestnut *Moore v. Regents of California*. *Moore* addressed a different commodification question—the issue of a person's property rights to his own body, not just information about his body.[127] But the court confronted several questions relevant to the issue of property rights in information. The opinions suggest, first, that even those who agree that property is appropriately conceived as a bundle of rights disagree on how many rights must be in the bundle for an asset to constitute "property." The opinions suggest, second, that even where there is a consensus on the values at stake with respect to the commodification of the self, we may not reach agreement on whether granting individuals property rights in their physical selves will further or defeat those values. Finally, the opinions—and Moore's underlying claim—suggest that sometimes it is others' use of an item for commercial or other value that makes a property "frame" seem appropriate for that item. Since the connection between value and property is tenuous, it is worth exploring how easily property can appear salient, especially since, as I will argue, the property frame may have significant costs.

A. *"Self" Control*

To state the obvious, a ton of information is available on the Internet. We are only too happy to be able to learn with but a few mouse clicks the name of Gambia's capital city (if you are interested, Banjul) or the phone numbers of our favorite restaurants or the costs and schedules of airplane flights between our home towns and wherever we intend to go for vacation.

But some information is different. I would neither expect nor want information about my particular medical history or current medical problems to be available to everyone on the Internet. Why not? For one thing, medical information is subject to duties of confidentiality, and its accessibility might suggest a breach of trust or fiduciary obligation by my physician, a breach that violates the terms of the special relationship under which I have entrusted my interests to her.[128] But violation of trust or other duties does not fully capture my concerns. I would be just as upset—indeed, probably more upset—about the disclosure of my medical information if it resulted from an unforeseen and unforeseeable hacking of my doctor's records by evil-doers using innovative technology against which my doctor could not reasonably

127. Moore did claim a right to be *informed* about his doctors' non-therapeutic interest in his cells. For the specifics of Moore's claims, see *infra* text accompanying notes 182–183.

128. Neil M. Richards & Daniel J. Solove, *Privacy's Other Path: Recovering the Law of Confidentiality*, 96 GEO. L.J. 123, 135, 157 (2007).

defend. In summary, with respect to personal information, I might have two related concerns: the first relates to what is public, and the second relates to how it became public.

The information in my medical record is, in a fairly straightforward sense, information about my "self." Other information related to my self is, of course, already available on the Internet. On the website of the law school for which I work, anyone can find a "profile" of me, including my resume, a brief narrative biography, and other "professional" facts such as a list of the conferences at which I have recently spoken.[129] In many ways, this information is different from the information in my doctor's EHR. One obvious difference is that I chose to disclose these particular facts about myself, as contrasted with the involuntary disclosure produced by physician carelessness or by hacking.

A second difference might appear to be that the information about my professional life is less sensitive or personal. But this distinction is hard to sustain. Because I have been a law professor for a very long time and because my work matters deeply to me, I care a great deal about both what information about my professional life is presented and how it is presented. Even if my law school had not already posted my CV to the web, I might not care much if a hacker invaded my computer files, found the résumé I created, and put it up on the Internet for all the world to see. And yet I might feel very differently if that same hacker posted, say, the rejections I have received from law reviews or an early draft of an article with a controversial, "half-baked" thesis. And surely I would be devastated if the hacker had found and posted, say, negative faculty recommendations related to my tenure and promotion, or unfounded student allegations of harassment. I would have just as strong an interest in controlling whether this information (or misinformation) about my professional "self" becomes available, and in what form, as I do in the information about my medical "self."

What we see here again is that medical information—which is "secret" and "sensitive"—is at least in some circumstances but an instantiation of the larger category of "personal information." Medical information clearly concerns the "self," but so does other information. In all instances, what we desire is control and what we fear is the loss of the power to define our selves.[130] This loss may occur through involuntary, unconsented to disclosure, e.g., where insufficient care is taken to safeguard information or where, as in hacking, the information is stolen notwithstanding responsible efforts

129. *Jane B. Baron Faculty Bio*, Temple University Beasley School of Law, http://www.law.temple.edu/Pages/Faculty/N_Faculty_Baron_Main.aspx (last visited Feb. 20, 2012).

130. Whether those who grew up in a time of pervasive social networking on sites such as Facebook will have the same concerns about self-control is a topic beyond the scope of this Article. For a brief consideration of the issues, see Mark A. Rothstein, *Health Privacy and the Facebook Generation*, The Hastings Ctr. Bioethics Forum (Aug. 11, 2009), *available at* http://www.thehastingscenter.org/Bioethicsforum/Post.aspx?id=3794.

to safeguard it. Or the loss may occur in more subtle ways, where we do not choose which non-confidential facts about ourselves are revealed or the way in which those facts are presented.

Should the law concern itself with these sorts of losses of "self" control? Some of these losses involve very tangible consequences. Identity theft is an obvious example. In such cases, the "self" who is buying or selling property, applying for or defaulting on loans, and the like, is literally not who she seems to be, and injures the "self" she has stolen by saddling her with unwanted debt, ruined credit, and other financial injuries.[131] Along the same lines, when one cannot control the "self" presented to an employer or to the world at large, one might lose employment opportunities or suffer injury to one's reputation.[132]

But tangible or actual injury may not exhaust the field of injury to self. We do not worry only about our monetizable assets, but also about controlling the construction of our identity. To the extent that out-of-control information threatens our ability, alone or with others, to create our own selves, it poses a threat we may ask the law to address. Should we have the legal power to control our "selves" in cyberspace? There are some powerful arguments in the affirmative.

In a variety of contexts, it has been argued that what it means to be a person is to invent[133] or author[134] one's own self, to create one's own narratives that organize disparate life events and experiences into coherent stories.[135] But the "digital person," created by unseen others out of one's credit card uses, mouse clicks, ATM withdrawals, and the like,[136] deprives individuals of the ability to create their own selves or author their own stories. The interest in self-invention or self-authorship might sound in

131. On the injuries of identity theft, see SOLOVE, *supra* note 5, at 109–19.

132. *See, e.g.*, Gostin, *supra* note 18, at 490. On the financial and reputation injuries that can be caused by insecure information, see generally Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477, 516–17 (2006).

133. *See* Eric J. Mitnick, *Procedural Due Process and Reputational Harm: Liberty as Self-Invention*, 43 U.C. DAVIS L. REV. 79, 117 (2009) ("[P]rotecting individual liberty entails securing to the greatest possible extent the free construction of the self and one's identity . . . . [L]iberty [is] self-invention.").

134. *See* Schwartz, *supra* note 52, at 1655 ("individuals who exercise self-determination . . . should be defined as people who, as part authors of their lives, substantially shape their existence through the choices they make"); Sean Hannon Williams, *Self-Altering Injury: The Hidden Harms of Hedonic Adaptation*, 96 CORNELL L. REV. 535, 554 (2011) (describing the self in terms of autonomy, "one core aspect" of which "is self-determination. . . . A person is self-determined to the extent that she is the author of her own ideals, goals and preferences.").

135. *See* Williams, *supra* note 134, at 568–70; *see also* ALASDAIR MACINTYRE, AFTER VIRTUE: A STUDY IN MORAL THEORY 217 (3d ed. 2007) (describing elements of a narrative sense of self); TAYLOR, *supra* note 124, at 47 (arguing that we make sense of our lives as stories).

136. *See* SOLOVE, *supra* note 5, at 1.

liberty,[137] autonomy,[138] or dignity.[139] Regardless, inability to create one's own self may be experienced as a serious loss.[140]

There is a different way to understand the self and the harm to self from uncontrolled flows of personal information. In this view, the development of individuality requires experimentation and deliberation, the opportunity to make—and possibly to regret—individual and social choices, and to derive from this process one's own beliefs, stances, and conceptions of the good.[141] But, some scholars argue, who would take intellectual, social, or creative risks if risk-taking were subject to constant scrutiny?[142] How could one try out a particular stance—toward politics, sexuality, or anything else—if the person one "inhabited" at one particular moment could be captured by others, who in effect might freeze it as one's identity for all time? If self-determination takes time[143] and practice,[144] then the constant monitoring of personal information will change the selves we develop.[145]

Alternatively, consider the possibility that the self is created socially, by reference to "rules of deference and demeanor," or "rules of civility," that command the forms of respect individuals are entitled to receive from others.[146] Under "the social norms that govern the flow of information in

137. Mitnick, *supra* note 133, at 117.

138. Williams, *supra* note 134, at 554.

139. *See* Kang, *supra* note 5, at 1260 (describing "dignity" as one of "the most fundamental reasons for respecting information privacy.").

140. In the medical context, self-creation can be problematic. A patient who moves to a new state might choose not to tell his new physician of past mental health, substance abuse, or sexual problems, and would thus author a story about himself that is inaccurate and inauthentic. Paper records do nothing to prevent this phenomenon. The interoperability of EHRs make this particular form of self-invention impossible. On the other hand, the information in the EHR will remain in the record permanently, and, as developed *infra* text accompanying notes 219–235, the interoperability of the electronic record may enhance the patient's vulnerability to disclosure and consequent desire for control of access to the EHR.

141. Cohen, *supra* note 6, at 1426.

142. *See* Solove, *supra* note 132, at 493 ("Surveillance can lead to self-censorship and inhibition."). Again, it is not clear whether this observation applies to a generation accustomed to constant self-exposure in social media.

143. Cohen, *supra* note 6, at 1424 ("[A]utonomous individuals do not spring full-blown from the womb.").

144. *See, e.g.*, Schwartz, *supra* note 7, at 2087 ("[D]eliberative democracy requires limits to access to personal information because Americans will hesitate to engage in democratic self-rule should widespread and secret surveillance become the norm."); Schwartz, *supra* note 52, at 1653 (arguing for limited access to personal data "to allow individuals, alone and in association with others, to deliberate about how to live their lives").

145. Cohen, *supra* note 6, at 1425–26 ("The point is not that people will not learn under conditions of no-privacy, but that they will learn differently . . . . Pervasive monitoring of every first move or false start will, at the margin, incline choices toward the bland and the mainstream."). Both Cohen and Schwartz worry about pressure towards conformity not only in terms of the loss to individuals, but the losses to the vitality of democratic deliberation, which requires well-developed, self-governing citizens. *See id*. at 1426–27; Schwartz, *supra* note 52, at 1658–66; Schwartz, *supra* note 7, at 2087.

146. *See* Robert C. Post, *The Social Foundations of Privacy: Community and Self in the Common Law Tort*, 77 CAL. L. REV. 957, 963–67 (1989).

modern society," individuals may appropriately expect, as a matter of respect, to control informational "preserves" or "territories."[147] These preserves or territories "provide a normative framework for the development of personality,"[148] and are thus "constitutive of human dignity."[149] Violation of civility rules, the failure to respect information preserves, thus injures the ability to develop one's own self.[150]

Obviously, none of these visions of the self is uncontroversial or complete. They are useful, however, in evaluating why disclosures of personal information might be troubling even in the absence of conventionally-recognized economic or reputational injury. And they provide a way to understand why individuals might care deeply about who controls both the amount and the form of personal information available about them. They give us, in other words, another reason to see why the category of property holds the potential for providing the sort of control individuals seek over their very "selves."

This vision of property as "self" control ties in with yet another influential view of property: the view that property can connect to "personhood."[151] In Margaret Jane Radin's influential *Property and Personhood* article, she asserted that "to achieve proper self-development—to be a *person*—an individual needs some control over resources in the external environment. The necessary assurances of control take the form of property rights."[152] The personhood view contemplates that "a person can be bound up with an external 'thing' in some constitutive sense."[153] Where that is appropriately the case,[154] property that is personal deserves a higher degree of protection than property that is merely fungible.[155]

Assuming information can be a thing,[156] a "resource in the external environment," it is clearly capable of being constitutive of the self in any of the ways described above. To the persons to whom information pertains, the information is personal in Radin's sense of the term, while to other persons—the data aggregators or others who use the information as a

147. *Id.* at 984.
148. *Id.* at 985.
149. *Id.* at 1008.
150. *Id.* at 1009 (suggesting such violations also signal a weakening of community ties).
151. Radin, *supra* note 125.
152. *Id.* at 957.
153. *Id.* at 960.
154. Radin concedes that "there is bad as well as good in being bound up with external objects" and that people can be bound up with objects "in the wrong way or to too great an extent." *Id.* at 961.
155. *Id.* at 986 ("[T]he personhood perspective generates a hierarchy of entitlements: The more closely connected with personhood, the stronger the entitlement."); *Id.* at 960 (explaining that fungible property, in this view, is property valued "for purely instrumental reasons.").
156. Smith, *Property and Property Rules*, *supra* note 98, at 1754 (including "intangibles" along with tangible "things").

commercial asset—the information is quintessentially fungible. Thus, to the subjects of information flows, data has a value different from the value it has to users of the information, and this value arguably warrants its protection "against cancellation by conflicting fungible property claims of other people."[157] Because personal information connects to personhood, we might give individuals property rights to control the flows of information about them.

Of course, Radin's theory of property and personhood is no less controversial than theories of property as involving consolidated, *in rem*, or bundles of rights.[158] To those who would base property rights on first possession,[159] it is not obvious why data aggregators do not already own the information in question.[160] To those who would base property rights on labor, it is again unclear that the subject of the information will have a better claim to own it than those who worked to collect it.[161] Finally, for those who define property in terms of efficiency-based market trades, it is not obvious why property rights in personal information should be held by the subjects of that information as opposed to those who value the information enough to have paid to acquire it.[162]

The point here is not that these more traditional theories of property are better than a personhood theory. Rather, the point is that, from these perspectives, "personhood" is not relevant to whether individuals have a property interest or not. In the absence of a single, accepted "meta"-definition of

---

157. Radin, *supra* note 125, at 1015.

158. *See supra* text accompanying notes 80–108.

159. On first possession, see Dean Lueck, *The Rule of First Possession and the Design of the Law*, 38 J.L. & Econ. 393 (1995); Joseph William Singer, *Original Acquisition of Property: From Conquest & Possession to Democracy and Equal Opportunity*, 86 Ind. L.J. 763 (2011).

160. *See* Cohen, *supra* note 6, at 1382 ("[P]ersonhood theory . . . seems an odd way of talking about my control over data that others already possess.").

In the absence of originality, the facts in databases are not eligible for copyright protection. *Feist*, 499 U.S. 340. Thus, data aggregators do not technically "own" the information that they compile. On the rights of data aggregators, see Daniel Gervais, *The Protection of Databases*, 82 Chi.-Kent L. Rev. 1109, 1135 (2007); Jacqueline Lipton, *Balancing Private Rights and Public Policies: Reconceptualizing Property in Databases*, 18 Berkeley Tech. L.J. 773, 814 (2003); Reichman & Samuelson, *supra* note 66, at 137. However, "the fact that . . . databases-as-compilations are not regarded by US law as property does not stop those who compile them from trading them . . . . The market effectively creates a property right where there is an impetus to deal commercially with the item in question, regardless of the stance a particular legislature might take on the creation of a property right." Jacqueline Lipton, *Mixed Metaphors in Cyberspace: Property in Information and Information Systems*, 35 Loy. U. Chi. L.J. 235, 251 (2003).

161. *See* Cohen, *supra* note 6, at 1381. The labor theory is conventionally traced back to Locke. John Locke, Two Treatises of Government 306 (Peter Laslett ed., Cambridge Univ. 1988) (1690).

162. *See* Cohen, *supra* note 6, at 1381; *see also* Richard A. Posner, Economic Analysis of Law 32–34 (7th ed. 2007) (stating that the role of property rights is to incentivize individuals to invest in their property and its most efficient use, with the assurance that they will recoup the costs incurred through wealth-maximizing transactions with others).

property, nothing guarantees that the personhood perspective will prevail. But if one believes that property *can* connect to personhood, and if one sees information about one's self as "personal" property in Radin's sense of that term, then one can plausibly argue that one's property interest in one's personal information has a special claim to legal protection—a claim that at the very least is superior to the claims of others, in whose hands the information is merely fungible. Were this argument to prevail, individuals' property rights would give them the ability to control both what information about them is made public and in what form. In this way, property for personhood might give rise to a right of "self" control.

B. *"Self" Commodification*

Let us assume that, based on concern for personhood (or some other concern), we grant individuals very simple property rights to information about themselves. Individuals would be able to keep information out of circulation altogether; information would be unavailable without its owner's consent. Individuals could also determine how information is presented by imposing conditions on disclosure. The "digital" self would be the self an individual chose to present, not a self constructed by others in secret. After all, if someone wants access to my bracelet or my copy of a rare first edition of *Great Expectations*, I must first agree to her use; why should access to my weight or history of law review rejections be any different? If someone wants what is mine, she must persuade me to sell it or give it away. The choice is mine to make. This is how property might give me "self" control: if I want you to have information about me, I'll sell or give it to you, and if I don't, I won't.

As we have seen, the "market" for information has potential problems, such as information asymmetries between sellers and buyers about the use to be made of information after its initial sale.[163] These problems might lead to adjustments in the freedom to make trades, i.e., to regulation of information markets. But, in the property paradigm, "self" control requires that the individual have *some* power over personal information, including the power to sell it, even if under limited conditions. Thus, we would have (some kind of) a market in personal information.

While markets for information make a good deal of sense in terms of "self" control, the notion of selling one's "self" is not entirely appealing. Morally, "self" selling seems troubling because it treats deeply personal, self-defining "goods" in personal information identically to every other "good," and reduces people to the sum of their sales.[164] Rhetorically, "self"

163. *See supra* text accompanying notes 69–72.

164. Radin, *supra* note 126, at 1861 (describing a regime of "universal market rhetoric" in which "everything that is desired or valued is conceived of and spoken of as a 'good,' " and in which "the person is conceived of and spoken of as the possessor and trader of these goods, and hence all human interactions are sales."). On the moral dimension of this observation, see

selling sounds bad—do we want to talk about the "self" in the same way we do unremarkable objects such as mousetraps or bath towels? Is it appropriate to commodify the self, i.e., to treat the self as a separate "thing" that can be traded?[165]

These concerns might seem overblown. The "property" in question is information—data—about persons. Surely persons are not constituted as selves solely in terms of data; they are not aggregates of facts such as their blood pressure, persistent back pain, or history of publication success or failure. To trade in information about the self is surely different from trading one's very self.

This argument is in some sense true—none of us is entirely the sum of all the facts that might be revealed about us. But it is also in some sense untrue. If there is anything to the idea of the digital person, we must take seriously that in cyberspace, we are created as selves precisely in terms of the aggregate of the uncountable facts of our phone calls, credit card transactions, age, voting record, mouse clicks, and the like. The self we seek to control via property is in fact constituted of data. In this sense it is, lamentably, the case that in selling personal information we sell our selves. Putting this point another way, it is hard to argue that data aggregators rob us of the ability to create our own selves and at the same time to argue that data about us is disconnected from our selves.

If we are to some extent our personal information, and if we are to control our selves by our decisions about trading that information, then our property rights in information will involve at least some commodification of our selves. For some theorists, this phenomenon is deeply problematic. As Radin puts it, "in our understanding of personhood we are committed to an ideal of individual uniqueness that does not cohere with the idea that each person's attributes are fungible, that they have a monetary equivalent, and that they can be traded off against those of other people."[166] To those who take this view, even talking about personal attributes in market terms is dangerous. In Radin's now-famous words:

> Market rhetoric, if adopted by everyone, and in many contexts, would indeed transform the texture of the human world. This rhetoric leads us to view politics as just rent seeking, reproductive capacity as just a scarce good for which there is high demand, and the repugnance to slavery as just a cost. To accept these views is to

---

Jane B. Baron & Jeffrey L. Dunoff, *Against Market Rationality: Moral Critiques of Economic Analysis in Legal Theory*, 17 CARDOZO L. REV. 431 (1996).

165. MARGARET JANE RADIN, CONTESTED COMMODITIES 58 (1996); Radin, *supra* note 125, at 966 ("We have an intuition that property necessarily refers to something in the outside world, separate from oneself."); *see also* Radhika Rao, *Property, Privacy, and the Human Body*, 80 B.U. L. REV. 359, 364 (2000) ("[P]roperty envisions a person who 'owns' and is thus distinct from his or her body . . . .").

166. Radin, *supra* note 126, at 1885.

> accept the conception of human flourishing they imply, one that is inferior to the conception that we can accept as properly ours.[167]

If personal information connects in important ways to our selves, then trading it has the potential to undermine our identity,[168] to alienate us (in both the property and psychological sense) from our selves.[169]

Again, though, we confront a fault line in property theory. As Landes and Posner's proposal for a market in babies illustrates, not everyone believes that commodification of even the most controversial "goods" is a bad thing.[170] More specifically, there is considerable disagreement over whether the commodification of identity is necessarily degrading.[171] In addition, some theorists resist the dichotomization of market and non-market realms, arguing that many interpersonal transactions have market elements and vice versa.[172] Perhaps commodification is just not a worrisome phenomenon.[173]

Moreover, even if we accept the view that commodification is at least potentially troubling as a moral or rhetorical matter, it is not entirely clear whether we should worry about the commodification of personal information. Concern about commodification is concern that the "wrong" things will be commodified; it does not worry us to trade mousetraps and bath towels. But it should worry us, commodification theorists argue, when we commodify the "many kinds of particulars—one's politics, work, religion, family, love, sexuality, friendships, altruism, experiences, wisdom, moral commitments, character, and personal attributes" that are "integral to the

---

167. *Id.* at 1884.

168. *Id.* at 1905 ("[U]niversal commodification undermines personal identity by conceiving of personal attributes . . . as monetizable and alienable from the self.").

169. *Id.* at 1907 (describing "two kinds of alienation" created when the personal is treated as fungible).

170. Elisabeth M. Landes & Richard A. Posner, *The Economics of the Baby Shortage*, 7 J. LEG. STUD. 323 (1978).

171. *See, e.g.*, Regina Austin, *Kwanzaa and the Commodification of Black Culture*, *in* RETHINKING COMMODIFICATION 178 (Martha M. Ertman & Joan C. Williams eds., 2005).

172. Joan C. Williams & Viviana A. Zelizer, *To Commodify or Not to Commodify: That is Not the Question*, *in* RETHINKING COMMODIFICATION, *supra* note 171, at 362, 368–69; *see also* Carol M. Rose, *Afterword: Whither Commodification?*, *in* RETHINKING COMMODIFICATION, *supra* note 171, at 402.

173. Radin's arguments about commodification have been critiqued on a variety of grounds. *See* Stephen J. Schnably, *Property and Pragmatism: A Critique of Radin's Theory of Property and Personhood*, 45 STAN. L. REV. 347 (1993) (arguing against Radin's notion that, without state-imposed restraints, commodification inevitably follows from market alienability); *see also* Neil Duxbury, *Law, Markets and Valuation*, 61 BROOK. L. REV. 657 (1995) (arguing that there is no uncontroversial way to define market-inalienable property); Peter Halewood, *Law's Bodies: Disembodiment and the Structure of Liberal Property Rights*, 81 IOWA L. REV. 1331 (1996) (arguing that personhood has been commodified in a variety of ways over time); Jeanne Lorraine Schroeder, *Virgin Territory: Margaret Radin's Imagery of Personal Property As the Inviolate Feminine Body*, 79 MINN. L. REV. 55 (1994) (arguing that market alienation creates community by enabling interactions among people, which fosters dependence on people instead of objects).

self."[174] To return to the observation that we are more than the sum of data available about us, it is not entirely clear that all or even much of the information about us in cyberspace is "integral" to the self in this sense. Radin admits that the line can be hard to draw: "there is no algorithm or abstract formula to tell us which items are (justifiably) personal. A moral judgment is required in each case."[175] Yet it is not clear that all would share moral judgments about which items of personal information it is improper to trade.[176]

Finally, even if we assume that commodification is potentially problematic, and that personal information is the kind of integral-to-self good that we should be particularly worried about trading, commodification may nonetheless be our fate. As Radin concedes, we live in a "nonideal" world.[177] We do not create a legal order on a clean slate, but must confront existing realities that change the valence of rights we might otherwise assert. In the case of information, the existing reality is that an unimaginable amount of information has already been collected about each of us, and that information is aggressively traded—is controlled—by data aggregators who are invisible to us. This reality creates a double bind analogous to the one described by Radin in respect of the sale of sexual services:[178] if we provide individuals property rights to personal information, we create the moral and rhetorical problems described above, but if we fail to provide individuals property rights to personal information, we enhance the power of others, in whose hands the information is solely a commodity. In the real world, information is already effectively commodified property, and the only question is whose.[179] But just as "property" alone cannot tell us what to treat as personal and what as fungible, "property" alone cannot decide who

174. Radin, *supra* note 126, at 1905–06.

175. *Id.* at 1908.

176. Putting this point another way, commodification theory does not tell us how to tell what are attributes of the self, or what we can and cannot appropriately separate from the self.

177. Radin, *supra* note 126, at 1915.

178. *Id.* at 1916–17 ("If we now permit commodification, we may exacerbate the oppression of women—the suppliers. If we now disallow commodification—without what I have called the welfare–rights corollary, or large-scale redistribution of social wealth and power—we force women to remain in circumstances that they themselves believe are worse than becoming sexual commodity–suppliers.").

179. *See* Richard S. Murphy, *Property Rights in Personal Information: An Economic Defense of Privacy*, 84 GEO. L.J. 2381, 2383–84 (1996) ("[Personal information,] like all information, is property. The question the law must answer is: Who owns the property rights to such information—the individual involved, the person who obtains the information, or some combination?"). As noted *supra* note 160, the legal status of data aggregators' rights to ownership of the information in their databases is not entirely clear.

Radin argues that in situations such as these, where "we cannot respect personhood either by permitting sales or banning sales, justice requires that we consider changing the circumstances that create the dilemma." Radin, *supra* note 126, at 1917. Nonetheless, she recognizes, "we still must chose a regime for the meantime." *Id*. Whatever that regime, information will be commodified.

should own commodified information. In both instances, a moral judgment is required.

C. *"Self" Ownership*

Much of the commodification debate has played out in connection with the issue of self-ownership in a literal sense: do we "own" our own physical bodies or parts thereof?[180] Many of those who entered law school after 1990 have encountered this issue in connection with *Moore v. Regents of the University of California*,[181] now a staple of almost every basic Property casebook.[182] In *Moore*, the plaintiff alleged that the use of his cells by others without his permission for potentially lucrative medical research constituted "conversion" of his property. In a wide-ranging opinion that evaluated both existing common law and its possible extension, the Supreme Court of California held that Moore had failed to state a cause of action for conversion, but that his complaint did state a cause of action for breach of fiduciary duty or lack of informed consent.[183] The opinion has much to teach about property's limits in deciding questions about control of the "self."

Moore's facts are simple.[184] Moore had hairy-cell leukemia, for which he was referred to Dr. David Golde, a physician at the University of California, Los Angeles. Golde performed a variety of tests on Moore's blood, bone marrow aspirate, and other bodily substances to confirm the diagnosis, and, for therapeutic reasons, ultimately removed Moore's spleen. Moore's complaint alleged that almost from the start of the treatment, Golde and the other defendants[185] believed that Moore's cells were of great scientific and commercial value, but did not disclose to Moore their plan to develop a commercially-valuable cell line from the tissue removed from Moore's body. To make matters worse, over the five years following the surgery, Golde directed Moore to return on several occasions, where additional

180. *See, e.g.*, Michele Goodwin, *Altruism's Limits: Law, Capacity, and Organ Commodification*, 56 RUTGERS L. REV. 305 (2004); Peter Halewood, *On Commodification and Self-Ownership*, 20 YALE J.L. & HUMAN. 131 (2008); Rao, *supra* note 165.

181. Moore v. Regents of the Univ. of Cal., 793 P.2d 479 (Cal. 1990). While the *Moore* case brought the issue of ownership of human tissue to the forefront of academic attention, it was neither the first nor the last instance in which human tissue was removed or used for research and commercial purposes without a patient's knowledge or consent. For the story of Henrietta Lacks, whose cells were removed, used, and commercialized without consent long before Moore's, see SKLOOT, *supra* note 16. For a more recent case involving allegations of unauthorized use of human tissue, see Greenberg v. Miami Children's Hospital Research Institute, Inc., 264 F.Supp.2d 1064 (S.D. Fla. 2003).

182. JESSE DUKEMINIER ET AL., PROPERTY 69 (7th ed. 2010); THOMAS W. MERRILL & HENRY E. SMITH, PROPERTY: PRINCIPLES AND POLICIES 255 (2007); SINGER, *supra* note 88.

183. 793 P.2d at 497.

184. The defendants demurred to the complaint, and so the case was decided entirely on the pleadings. *Id.* at 480.

185. The other four defendants were the Regents of the University of California, who owned and operated the hospital; Shirley G. Quan, a researcher employed by Regents; Genetics Institute, Inc.; and Sandoz Pharmaceuticals Corporation and related entities. *Id.* at 480–81.

samples of blood and tissue were removed—possibly without any medical reason and definitely without disclosure to Moore that the removed cells would be used for research purposes. Ultimately, the efforts of Golde and the other defendants resulted in a new, patented cell line, allegedly worth over three billion dollars.

The court's opinion totals nearly fifty pages in length.[186] Professors teaching first year law students could not have ordered up a better introduction to the building blocks of legal argumentation, as the majority opinion rejects the conversion claim on grounds of common law and statutory doctrine, of policy, and of institutional competence. Much could be and has been written about the case,[187] but I focus here on three of its aspects that relate directly to the question of property in personal information: the opinions' examination of "self"-ownership, of the perils of "self"-commodification, and of the possibility that Moore's property claims might rest on or derive from the value that *others* had obtained from his cells and tissue.

Moore's claims to self-ownership arose in a legal landscape cluttered by public health statutes governing such matters as organ donation, blood procurement, and, most importantly for Moore, tissue disposal.[188] The statute on tissue disposal,[189] which required that "following conclusion of scientific use" human tissues be disposed of "by interment, incineration," or other

186. This total includes one concurring opinion, one opinion concurring in part and dissenting in part, and one dissent.

187. *See, e.g.,* Benjamin Appelbaum, Moore v. Regents of the University of California*: Now that the California Supreme Court Has Spoken, What Has It Really Said?*, 9 N.Y.L. SCH. J. HUM. RTS. 495 (1992) (analyzing *Moore* in terms of the case's impact on the scientific community); Karen G. Biagi, Moore v. Regents of the University of California: *Patients, Property Rights, and Public Policy*, 35 ST. LOUIS U. L.J. 433 (1991) (arguing that the public policy arguments on which the court based its decision are outweighed by the patient's right to assert a commercial interest in his tissues); Anne T. Corrigana, *A Paper Tiger: Lawsuits Against Doctors for Non-Disclosure of Economic Interests in Patients' Cells, Tissues and Organs*, 42 CASE W. RES. L. REV. 565 (1992) (evaluating whether the causes of action *Moore* recognized effectively protect patients' interests); K. Peter Ritter, Moore v. Regents of the University of California: *The Splenetic Debate Over Ownership of Human Tissue*, 21 SW. U. L. REV. 1465 (1992) (arguing that human body parts and tissues can be treated as a form of tangible personal property). These articles are merely illustrative; hundreds of law review articles cite and discuss *Moore*.

188. "[T]he laws governing such things as human tissues, transplantable organs, blood, fetuses, pituitary glands, corneal tissue, and dead bodies deal with human biological materials as objects sui generis . . . . It is these specialized statutes, not the law of conversion, to which courts ordinarily should and do look for guidance on the disposition of human biological materials." 793 P.2d at 489.

189. "Notwithstanding any other provision of law, recognizable anatomical parts, human tissues, anatomical human remains, or infectious waste following conclusion of scientific use shall be disposed of by interment, incineration, or any other method determined by the state department to protect the public health and safety. As used in this section, 'infectious waste' means any material or article which has been, or may have been, exposed to contagious or infectious disease." CAL. HEALTH & SAFETY CODE § 7054.4 (2011).

approved methods, proved particularly problematic for Moore. As the majority interpreted the statute:

> One cannot escape the conclusion that the statute's practical effect is to limit, drastically, a patient's control over excised cells. By restricting how excised cells may be used and requiring their eventual destruction, the statute eliminates so many of the rights ordinarily attached to property that one cannot simply assume that what is left amounts to "property" or "ownership" for purposes of conversion.[190]

In the majority's view, then, the legislature had spoken, and while "the Legislature did not specifically intend this statute to resolve the question of whether a patient is entitled to compensation for the nonconsensual use of excised cells,"[191] it had so depleted the rights in the patient's bundle that what remained could not plausibly be called "property."

In dissent, Justice Mosk took direct issue with the majority's conclusion. After specifically referring to the view of property as a bundle of rights, Mosk noted that "the same bundle of rights does not attach to all forms of property."[192] He then listed a variety of limitations routinely imposed on property interests, including time, place, and manner-based limits on use, restrictions on sale, restrictions on gifts, and wholesale restraints on alienability.[193] These limitations, he argued, did not render the remaining interest too weak or empty to be called property: "The limitation or prohibition diminishes the bundle of rights that would otherwise attach to the property," Mosk wrote, "yet what remains is still deemed in law to be a protectable property interest."[194]

Notice that the majority and the dissent did not disagree on the relevant theory or definition of property; this was not a dispute as to whether property rights are best characterized as standardized rights *in rem* or as bundles of rights.[195] Both the majority and the dissent were willing to analyze Moore's conversion claim through a bundle of rights frame. However, their agreement on what property theory to apply was not sufficient to bring them into accord; they could not reach consensus on how many rights must be in the bundle for a "property" claim to survive. This disagreement bodes ill for those who look to the field of property to provide definite answers to new questions involving control of personal information.

The same pattern of agreement on first principles, but disagreement on their application, can be seen in the *Moore* opinions' treatment of the problem

---

190. 793 P.2d at 491–92.
191. *Id.* at 491.
192. *Id.* at 509.
193. *Id.* at 510.
194. *Id.*
195. *See supra* text accompanying notes 81–84, 86–108.

of commodification. Justice Arabian, concurring, wrote to "speak of the moral issue,"[196] which he defined as follows:

> Plaintiff has asked us to recognize and enforce a right to sell one's own body tissue *for profit*. He entreats us to regard the human vessel—the single most venerated and protected subject in any human society—as equal with the basest commodity. He urges us to commingle the sacred with the profane. He asks much.[197]

Because Justice Arabian could not be sure whether treating human tissue as "a fungible article of commerce" would "uplift or degrade" the "unique human persona,"[198] he agreed with the majority that the decision was best left in legislative hands.[199]

Justices Mosk and Broussard both dissented on this exact point. Justice Mosk agreed that "our society acknowledges a profound ethical imperative to respect the human body as the physical and temporal expression of the unique human persona."[200] But that respect, Justice Mosk argued, was on equitable as well as ethical grounds best manifested by recognizing "that every individual has a legally protectable property interest in his own body and its products."[201] Justice Broussard was even more forceful with respect to the issue of commodification:

> The majority's rejection of plaintiff's conversion cause of action does *not* mean that body parts may not be bought or sold . . . or that *no* private individual may benefit economically from the fortuitous value of plaintiff's diseased cells. Far from elevating these biological cells above the market place, the majority's holding simply bars *plaintiff*, the source of the cells, from obtaining the benefit of the cells' value, but permits *defendants*, who allegedly obtained the cells . . . by improper means, to retain and exploit the [cells'] full economic value.[202]

As with the question of the applicable theory of property, the justices on both sides did not disagree on fundamental principles: the body is special, and treating it as an ordinary good is problematic. But this agreement on the dangers of commodification did not bring the justices into accord. In Justice Arabian's view, respect for the unique nature of the human body counseled *against* a grant of property rights, while the identical respect, in Justice Mosk's view, counseled *for* a grant of property rights. Meanwhile, Justice Broussard focused on the inevitability of commodification: the cells, he ar-

196. 793 P.2d at 497.
197. *Id.* at 498.
198. *Id.* at 497–98.
199. *Id.* at 498.
200. *Id.* at 515.
201. *Id.*
202. *Id.* at 506.

gued, would be someone's property, and the only question was whose. Like property theory, commodification theory provides no clear answers to ownership of the physical self, and is thus unlikely to lead to clear answers to ownership of information about the self.

There is yet another way in which *Moore* sheds light on the possibilities for using property as a vehicle to control personal information, and it derives from Moore's posture with respect to his own tissues before he knew that defendants had utilized them to form a commercially valuable cell line. It seems unlikely that, on his own, Moore would have kept the cancerous cells, enlarged spleen, or blood samples that were removed from his body; how much use would they have seemed to him? Indeed, had the defendants not developed a commercially-valuable product out of Moore's cells, it is hard to imagine him asserting a conversion claim. How many of us, who have had blood samples taken in a doctor's office or a hospital, or who have donated blood, have thought of that blood as our "property"?[203] Yet once Moore understood that his tissue and cells had value in the hands of others, "property" became a salient frame for him. In other words, the cells might not have seemed "property" to him when they were withdrawn, but once he saw their value as property to others, he saw his cells in a different way—not as useless items for which he had no need, but as his property.[204]

The association between "value" and "property" is, of course, not one of logical entailment; it is only after an asset has been recognized as legally protectable property that it will have commercial value.[205] Yet, however naïve,

---

203. Which is not to say that we do not think of it as "our" blood. We do. And we would, for this reason, be angry if the laboratory to which the blood was sent mishandled the blood, confusing "our" blood with another's. But we would not necessarily see the harm of mishandling as a "property" problem.

204. This aspect of Moore's claim is somewhat obscured in the court's opinions by a complicated and confusing discussion of what, exactly, made Moore's cells valuable. By the time the case arose, the defendants had patented the cell line they had developed from Moore's tissue and, since naturally occurring substances are not patentable, Diamond v. Chakrabarty, 447 U.S. 303 (1980), the majority reasoned that the "property" in question must have derived from something other than the raw materials Moore contributed. In the eyes of the majority, the value of Moore's cells derived from the defendant's "incentive effort" in transforming Moore's cells—effort that had to have been made for the patent to have lawfully issued. As the majority put it, "Moore's allegations that he owns the cell line . . . are inconsistent with the patent, which constitutes an authoritative determination that the cell line is the property of the invention." 793 P.2d at 492. But the majority somewhat undermined this reasoning in another part of its opinion where, to rebut the claim that Moore must have had an interest in his unique genetic materials, it found that the lymphokines defendants had manufactured "have the same molecular structure in every human being" and were not unique to Moore. *Id.* at 490.

205. *See* United States v. Willow River Power Co., 324 U.S. 499, 502 (1945) ("[N]ot all economic interests are 'property rights'; only those economic advantages are 'rights' which have the law back of them, and only when they are so recognized may courts compel others to forbear from interfering with them or to compensate for their invasion."); Int'l News Serv. v. Associated Press, 39 U.S. 215, 246 (1918) (Holmes, J., dissenting) ("Property, a creation of law, does not arise from value, although exchangeable—a matter of fact. Many exchangeable

Moore's claim seemed quite plausible to the dissenting justices. In rejecting the majority's assertion that patients such as Moore would be sufficiently protected by disclosure of physicians' potentially-conflicting research interests, Justice Broussard noted that the majority "fails even to mention the patient's interest in obtaining the economic value, if any, that may adhere in the subsequent use of his own body parts."[206] Justice Mosk made a similar point. Responding to the argument that the tissue disposal statute had deprived Moore of so many rights that no property remained in the bundle, Mosk wrote that "Moore nevertheless retained valuable rights in that tissue. Above all, at the time of its excision he at least had *the right to do with his own tissue whatever the defendants did with it*."[207] Both dissenting justices, then, basically took the exact position that Moore did: that however little "property" might have existed in these tissues before their commercial potential became known, plenty of property existed afterwards.

There are obvious parallels between Moore's claims to property rights in his excised tissue and claims to property rights in personal information. Like Moore's cells, in our own hands our information doesn't seem much like property. There is a lot of personal information about which, on our own, we might not much care (did I use the ATM at the Market Square shopping center or the ATM at the University?; did I weigh the same at my last doctor's visit as I weigh today?; did I use Expedia or the US Airways website to book my two most recent flights?). This isn't to say that some of the information or its patterns might not be of interest; many people keep close track of their cash flow each month, their weight, or their vacation costs. But even when we pay attention, we might not be apt to characterize our interest in information in terms of "ownership." But, as happened to Moore, once we learn that others are capitalizing on information about us, it becomes much easier to think of it as "ours," as "property" that others have "taken" from us.

How are we to explain this shift in our characterization of these "goods," the moment when property becomes salient? One explanation would call upon what Radin calls the "domino theory,"[208] under which "once something is commodified for some it is willy-nilly commodified for every-

---

values may be destroyed intentionally without compensation. Property depends upon exclusion by law from interference.").

This point raises obvious issues well beyond the scope of this Article respecting the relationship between property and the state. The claim I make here is a limited one, which is that, absent legal protection, individuals cannot reliably extract economic value from what they might have otherwise considered "assets" because they cannot keep others from using those assets.

206. 793 P.2d at 505. In Broussard's eyes, the patient would be entitled to that value even if it constituted a "fortuitous 'windfall' " to the patient. *Id.*

207. *Id.* at 510. Mosk went on to note that "the majority cite no case holding that an individual's right to develop and exploit the commercial potential of his own tissue is not a right of sufficient worth or dignity to be deemed a protectable property interest." *Id.*

208. Radin, *supra* note 126, at 1909.

one."[209] The idea here is that the rhetoric of the market is difficult to control; its introduction in one sphere (data aggregation and sale) may bleed into other spheres, making it impossible for us to think of those other spheres in non-commodified ways.[210] So, in *Moore*, once the defendants began to speak of Moore's cells in terms of their commercial potential, it became impossible for Moore to think or speak of them in noncommercial terms. And so, in terms of personal information, once we realize that others are already using information about us in lucrative ways, it becomes impossible for us to think or speak of that information except in terms of its market value.[211] This would be one way to understand how and why we see shifts from non-property to property frames.

Another way to understand how and why we see such shifts is in terms of property's "relativity." It is a widely accepted view of property, especially under the bundle-of-rights view, that property rights can be relative, dependent on the particular relationship between various parties. A standard example is that of a prior possessor without proof of title—a finder—who is considered to have a property right that would prevail against all later comers, including bailees and thieves, but not against the true owner of the found object.[212] Something similar to this sort of thinking is illustrated in Justice Broussard's dissent in *Moore*. Responding to the majority's argument that removed body parts could not be property for any purpose, Broussard proposed a counter-factual:

> If, for example, another medical center or drug company had stolen all of the cells in question from the UCLA Medical Center laboratory and had used them for its own benefit, there would be no question but that a cause of action for conversion would properly lie against the thief . . . . Thus, the majority's analysis cannot rest on the broad proposition that a removed body part is not property, but rather rests on the proposition that *a patient* retains no ownership interest in a body part once the body part has been removed from his or her body.[213]

Justice Mosk's argument—that Moore had "*the right to do with his own tissue whatever the defendants did with it*"[214]—is consistent with what seems to be Broussard's point. Perhaps for some purposes, we might deny

209. *Id.* at 1914.

210. *Id.*

211. The domino effect is not inevitable. Radin concedes that there are cases where the introduction of the rhetoric of commodification might not lead to the inability to think of the good in question in noncommodified ways. *Id.* She argues that "we should evaluate the domino theory on a case-by-case basis." *Id.*

212. *See, e.g.*, Tapscott v. Lessee of Cobbs, 52 Va. 172 (11 Gratt. 172) (1854); Armory v. Delamirie, 93 Eng. Rep. 664 (K.B. 1722).

213. Moore v. Regents of the Univ. of Cal., 793 P.2d 479, 501 (Cal. 1990).

214. *Id.* at 510.

that individuals own their tissue or their personal information. But with respect to other persons claiming to own those individuals' bodily tissue or information, the situation has changed; the individuals should have rights just as good against the world as the commodifiers of their tissue or their personal information might have.

Or perhaps the explanation of how property becomes salient derives from something as simple as envy. If a child who otherwise despises dolls and who is happily playing with paints asserts after she sees her brother begin to play with a neglected Raggedy Ann that the doll is "mine," we are not surprised. But it is not only children who, when they see others making use of what they themselves have ignored, discover an appetite to use the thing themselves—or at least get some compensation for its use. On this theory, property rights in personal information seem appropriate just when—and just because—others are seen to have them.[215]

However property frames might arise, they come at a cost. Once Moore conceptualized his interest in terms of property, he rather quickly jumped to the conclusion that he had the power to control the use of his tissue.[216] As with value, the connection between property and control is not one of logical entailment; owners are not in fact free to do just whatever they like with their property.[217] But again, lest Moore's claim be dismissed as naïve, it should be noted that a critical part of Justice Broussard's dissent was based on his belief that the majority's informed-consent and breach of fiduciary duty theory would not provide the kind or degree of control provided by conversion.[218] Once property enters the picture, it is all too easy to believe

---

215. This might be one perspective through which to view a case such as *Sorrell v. IMS*, 131 S. Ct. 2653 (2011). In any physician's individual hands, her prescribing data was not worth much; aggregated in the hands of commercial entities, the data was extremely valuable for marketing purposes—purposes the legislature later sought to proscribe in the statute at issue in the case.

The children's toy analogy makes the problem of the property frame both vivid and accessible, but the analogy should not be pushed too far. In the cases of both John Moore and Henrietta Lacks, there were elements of deceit by physicians of patients who had no way to know of the use being made of their cells, and the wrong in these cases is in this sense somewhat different than that experienced by the sister in the doll hypothetical. But in *Moore*, the patient claimed not only lack of informed consent and violation of fiduciary duty—claims based on deceit—but also conversion—a claim based on property.

216. "Moore . . . theorizes that he continued to own his cells following their removal from his body, at least for the purpose of directing their use[.]" 793 P.2d at 487.

217. Even fee owners' rights are limited by common law duties of reasonable use, by locally imposed zoning restrictions, and by easements and servitudes, just to name a few limits on owners' control powers. And of course non-fee owners such as tenants have even less control. As is developed *infra* text accompanying notes 259–262, unconstrained power—total control—is the exception, not the rule.

218. Judge Broussard wrote:

> As a general matter, the tort of conversion protects an individual . . . against unauthorized use of his property or improper interference with his right to control the use of his property. . . . [T]he complaint alleges that, before the body part was re-

that control ineluctably follows. As the next Part explains, this vision is as misleading as it is seductive.

III. Information's Future

For most of this Article, I have treated medical information as but a subset, a distinct category, of information generally. My argument has been that medical and other information is in at least one important way alike: it is information over which individuals seek control. It is control, I have argued, that has led to calls for the propertization of information.

In Section A of this Part, I survey some of the problems particular to health information. The survey does not purport to be complete. Its purpose is to highlight just a few of the many important *health* policy issues raised by the digitization of medical information. Even a cursory view of such issues suggests that the common law of property will be inadequate to cope with the many-faceted problems that arise with respect to digitized medical information. The solutions, if there are solutions, are more likely to be developed legislatively and administratively, and to be finely tailored to address a wide variety of distinct problems. While patients may be given some powers over the information collected about them, it is unlikely that those powers will look much like property in any of the senses in which that term is conventionally used.

In Section B, I suggest that the solution to the larger problem of information control also lies in legislation and regulation. Barely a day goes by that we do not read of catastrophic breaches of data security. If banks, credit card companies, cell phone carriers, and even the mighty Google cannot safeguard our personal information, surely at some point Congress will be pressured to act. Europe has already done so. We cannot know whether the resulting legislation will be effective in actually securing personal information. It will, however, be important expressively, evidencing public concern over uncontrolled disclosures of private information. Here again, property will play only a bit part in the solution.

In Section C, I argue that, in the context of information, property talk can mislead. At least some of the arguments for property rights in information rely on a somewhat simplistic association between property and "dominion." But even with respect to physical assets, property often gives owners far less control than is conventionally recognized. Indeed, the extent to which property implies control is deeply debated within property theory. In our increasingly interconnected world, we need to make difficult choices about how power and control should be allocated—and, most likely,

---

moved, defendants intentionally withheld material information that . . . was necessary for his exercise of control over the body part.

793 P.2d at 502.

shared—among a variety of parties. The concept of "property" alone cannot tell us how to make those choices.

A. *The Peculiar Problems of Medical/Health Information*

Medical information presents some unique policy challenges. The advantages of digitization require widespread adoption of EHRs, which must be made interoperable if they are to have the network effects that would lead to widespread improvement of outcomes. But adoption is expensive[219] and it is disruptive.[220] Interoperability requires standardization of data collection and interchange protocols.[221] And network effects require interconnection and coordination.[222] The market itself has not produced these "goods."[223] If it had, it would be hard to explain the creation of subsidies for EHR adoption,[224] the appointment of a National Coordinator for Health Information Technology within the Department of Health and Human Services,[225] and the use of such entities as the Institute of Medicine to formulate recommendations as to EHR use.[226]

Widespread adoption, if achieved, would create a raft of other issues. Will providers be liable for the errors of others who participate in the creation of a medical record?[227] For their own data input errors?[228] For failure to

219. Hall, *supra* note 7, at 639 (reporting cost estimates of $100 to $300 billion for a complete, nationwide system); Adam Seth Litwin, *Why Don't Docs Digitize? The Adoption of Health Information Technology in Primary Care Medicine* (Soc. Sci. Research Network, Paper No. 1431202, 2009), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1431202 (suggesting that even direct subsidies will not promote adoption unless physicians can share in the saving generated by ERH adoption).

220. Richard J. Baron et al., *Electronic Health Records: Just Around the Corner? Or Over the Cliff?*, 143 ANN. INTERN. MED. 222, 223–25 (2005) (describing the training, work-redesign, and financial burdens of EHR adoption).

221. *See, e.g.*, Nancy Ferris, *Electronic Health Record Standards*, HEALTH POLICY BRIEF, Sep. 28, 2010, at 1, *available at* http://www.healthaffairs.org/healthpolicybriefs/brief_pdfs/healthpolicybrief_26.pdf ("Another key goal is to make certain that data collected by one system is compatible with data collected by another.").

222. Hall, *supra* note 7, at 638.

223. *Id.* at 636 (describing "market failures" that led to government intervention).

224. *See* COMM. ON QUALITY OF HEALTH CARE IN AM., *supra* note 18.

225. In 2004, the Bush administration established the position of the National Coordinator for Health Information Technology in DHHS. *See* Laura Landro, *The Informed Patient: Electronic Medical Records Are Taking Root Locally*, WALL ST. J., Sept. 22, 2004, at D7; Steve Lohr, *Government Wants to Bring Health Records into Computer Age*, N.Y. TIMES, July 21, 2004, at C4; *see also* CONG. BUDGET OFF., *supra* note 21, at 3; *Farzad Mostashari, MD, ScM, National Coordinator for Health Information Technology*, OFF. OF THE NAT'L COORDINATOR FOR HEALTH INFO. TECH., http://www.healthit.gov/providers-professionals/farzad-mostashari-md-scm (last visited Feb. 21, 2012).

226. *See* COMM. ON QUALITY OF HEALTH CARE IN AM., *supra* note 18.

227. Sharona Hoffman & Andy Podgurski, *E-Health Hazards: Provider Liability and Electronic Health Record Systems*, 24 BERKELEY TECH. L.J 1524, 1542–44 (2009).

228. *Id.* at 1544–45.

read the entire longitudinal record before making recommendations?[229] For failing to properly follow security protocols?[230]

And what is the status of the information in EHRs? Many of the benefits of digitization contemplate the aggregation of data in multiple records. The data could then be used to improve public health, by identifying, for example, what percentage of patients experience adverse reactions to a specific drug, or how patients respond to alternative therapies.[231] But the aggregation of data and its use for public health purposes raise their own issues. Must the data in each record be "de-identified" and, if so, what is the best way to do so?[232] Should the data be considered a public good that should be owned by the public?[233] Should patients be able to opt out of data aggregation?[234]

These questions do not begin to exhaust the field of issues raised.[235] They do, however, illustrate the breadth of problems to be confronted, and the number of technical issues that will have to be addressed, if EHRs are to achieve their potential to change the delivery of health care. Even a cursory examination of the issues suggests that generally speaking they are not amenable to resolution by adjudication under common law property principles. Such principles tell us nothing about protocols for information exchange, de-identification, or aggregation. The will to set standards, and the expertise to set them effectively, must come from Congress or, more likely, the administrative agencies charged with delivering and paying for health care services.

EHRs are, after all, *health* records, and thus raise issues of health policy. With respect to these issues, it is not clear that "property" as a legal category has much to add. Let us assume for a moment that patients *do* have property rights in their medical information and that that right affords them some degree of control over the data in their EHRs. We might then decide as a policy matter that patients should have some powers over the data in their files, such that they could either access that data or have a voice in its use by

229. *Id.* at 1537–42.

230. As noted *supra* text accompanying note 45, one complaint about HIPAA is that it does not provide a private right of action.

231. On the public health benefits of EHRs, see Rodwin, *supra* note 7; Rodwin, *supra* note 29.

232. On deidentification, see Rothstein, *supra* note 4; *see also* KHALED EL EMAM ET AL., THE CASE FOR DE-IDENTIFYING PERSONAL HEALTH INFORMATION (2011), *available at* http://ssrn.com/abstract=1744038.

233. Rodwin, *supra* note 7, at 86, 88.

234. Evans, *supra* note 7, at 96. If patients could freely opt out of data aggregation, their individual control/veto rights could pose the danger of a health information anti-commons. Rodwin, *supra* note 7.

235. For example, how should employers treat data in EHRs? *See* Sharona Hoffman, *Employing E-Health: The Impact of Electronic Health Records on the Workplace*, 19 KAN. J.L. & PUB. POL'Y 409, 410–12 (2010) (surveying the issues that EHRs raise for employers). Should the data be made available to law enforcement officials? *See* 45 C.F.R. 164.512(f)(2010) (permitting disclosure of health information to law enforcement officials under specified circumstances).

others. It is nonetheless likely that patients' control rights would have to be highly qualified to account for, *inter alia*, the needs of system operability or the government's interest in public health. The solution to the myriad health policy problems that EHRs present is likely to involve numerous finely-grained rules focused on particularized problems. In the end, patients will have those powers—and only those powers—that are consistent with the other needs of a workable health system. Maybe those powers will resemble the powers we associate with "ownership" of "property," and maybe they won't. If they do, the category "property" will have had little to do with the matter. Health, reimbursement, and technical imperatives will all be more determinative.

B. *The More General Problem of Personal Information*

Not all personal information implicates exactly the same health, reimbursement, and technical issues presented by EHRs. But, as with medical information in particular, personal information is subject to a variety of conflicting forces and policy imperatives. On the one side, information is big business, and attempts to regulate its collection wholesale are likely to encounter significant resistance.[236] On the other side, each week brings a new story of information in danger—of systems breached or hacked; of credit card and social security numbers no longer secured.[237] The pressure to do something to protect personal information can only grow.

---

236. Lemley, *supra* note 66, at 1547–48 (arguing that well-financed collector/users of private information will work hard to block efforts to give property rights to individuals).

237. A breach at CardSystems Solutions, a company that processes more than fifteen billion dollars in credit card payments, exposed more than forty million credit card accounts of all brands. Citigroup lost nearly four million unencrypted consumer records stored on magnetic computer tapes during a shipment to a credit-reporting agency. Eric Dash & Tom Zeller, Jr., *Mastercard Says 40 Million Files are Put at Risk*, N.Y. TIMES, June 18, 2005, at A1. Another processing company, Heartland Payment Systems, suffered a breach potentially exposing tens of millions of credit and debit cardholders to the risk of fraud. Eric Dash & Brad Stone, *Big Breach In Card Data Raises Risk For Millions*, N.Y. TIMES, Jan. 21, 2009, at B4. The names, birth dates, and Social Security numbers of as many as 2.6 million veterans were exposed to identity theft when an intruder stole electronic data from a VA analyst's home in 2006. *See* Christopher Lee, *Veterans Angered by File Scandal*, WASH. POST, May 24, 2006, at A21; Hope Yen, *VA Didn't Alert FBI for 2 Weeks after Data Heist*, CHI. TRIB., May 24, 2006, at C4.

Epsilon, an online marketer that manages customer databases and email marketing for about 2,500 companies, suffered an unauthorized entry into its customer database, one of the largest database breaches in U.S. history. Though no financial information was compromised, the email information obtained could be used for "phishing," in which fraudulent e-mails request customers' account numbers, Social Security numbers, etc. *See Email-Theft Victims Still Coming to Light*, CHI. TRIB., Apr. 7, 2011, at C26; James Covert, *Massive E-Breach Targets Consumers*, N.Y. POST, Apr. 4, 2011, at 25.

The Department of Health and Human Services posts breaches of unsecured protected health information affecting more than five hundred individuals on their website. *See* U.S. Dep't of Health & Human Servs., *Breaches Affecting 500 or More Individuals*, HEALTH INFO. PRIVACY,

Europe has tackled the problem of controlling information by legislation. In 1995, the European Union issued its Directive on the Privacy of Personal Data 95/46/EC ("the Directive").[238] The specifics of the Directive are well beyond the scope of this Article, and already there are proposals for its revision.[239] Very roughly, the Directive sets objectives for handling personal data,[240] including fair and legal processing,[241] collecting and using data for "specified, explicit, and legitimate" purposes,[242] and maintaining accurate and complete records.[243] Processing under the Directive is narrowly constricted to when the data subject, the person to whom the information relates, gives unambiguous consent,[244] or specific instances of necessity.[245] Certain "special categories" of data[246] are afforded additional protection, and this sensitive data is prohibited from being processed,[247] with few exceptions.[248]

---

http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html (last visited Mar. 19, 2012). In general, there were so many data breaches in 2011 that some commentators refer to 2011 as the "Year of the Data Breach." *See* Michael P. Voelker, *After 'Year of the Data Breach,' Carriers Increase Capacity, Competition for Cyber Risks*, PROP. CASUALTY 360° (Feb. 2, 2012), http://www.propertycasualty360.com/2012/02/02/after-year-of-the-data-breach-carriers-increase-ca?t=commercial.

238. Council Directive 95/46/EC, 1995 O.J. (L 281) 31 (EU), *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML [hereinafter Directive].

239. Rebecca Wong, *Data Protection: The Future of Privacy*, 27 COMPUTER L. & SEC. REV. 1–5 (2011), *available at* http://works.bepress.com/cgi/viewcontent.cgi?article=1012&context=rebecca_wong&sei-redir=1#search=%222011+revision+to+95/46/EC%22.

240. Directive, *supra* note 238, at art. 6.

241. *Id.* at art. 6(1)(a). Processing is defined as "any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction." *Id.* at art. 2(b).

242. *Id.* at art. 6(1)(b).

243. *Id.* at art. 6(1)(d).

244. *Id.* at art. 7(a).

245. *See id.* at art. 7 (stating that instances of necessity include: creation or performance of a contract involving the data subject, compliance with a legal obligation, protection of data subject's vital interests, performance of a task in the public interest or with official authority, or legitimate interests of the controller or third party that override the interests of the data subject).

246. *Id.* at art. 8(1) (including information that reveals "racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership," and information regarding one's health or sex-life).

247. *Id.*

248. *Id.* at art. 8 (exceptions include: data subject gives explicit consent, processing is necessary for obligations and rights in the field of employment law or to protect "vital interests" of the data subject, processing is done as a legitimate activity of an association and relates solely to the members of that association, or processing relates to data the data subject makes public or to a legal claim).

Europe and America differ in many important respects in their attitudes toward and cultures of information.[249] The First Amendment alone might make Americans more suspicious than Europeans of the very idea of restrictions on information processing.[250] Putting this suspicion to one side, American regulation of information might differ from the Directive's provisions in many specific respects.

That said, it is hard to deny the appeal of a legislative solution to the problem of personal information, a solution that—like the Directive—attempts to be comprehensive and to unify the law. Sooner or later it seems likely that the U.S. will be pressured to move in this direction. As noted earlier, Congress has already enacted piecemeal legislation addressing narrow categories of information.[251] But the recent information-loss scandals range broadly, touching banks, mobile phone companies, and Google.[252] At some point, the problem will cry out for comprehensive resolution.

As with medical records, that resolution will need to encompass a number of interests: individuals care about nondisclosure of facts deemed sensitive, institutions care about the financial and practical burdens of protecting data, and the government cares about access to information it regards as necessary for national security or other "public" purposes.[253] Though po-

---

249. *See, e.g.*, James Q. Whitman, The Two Western Cultures of Privacy: Dignity Versus Liberty, 113 YALE L.J. 1151 (2004) (contrasting American and European cultures of privacy).

250. *See, e.g.*, 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).

251. *See* Terry, *supra* note 33.

252. *See, e.g.*, Dash & Stone, *supra* note 237. Apple and Google both have had recent incidences of security breaches. The AT&T network that supports Apple iPhones and iPads devices was hacked in 2010, exposing an estimated 114,000 user e-mail addresses. *See* Cecilia Kang, *Post Tech: Security Tech Exposes iPad Information*, WASH. POST, June 10, 2010, at A11; Miguel Helft, *AT&T Said to Expose iPad Users' Addresses*, N.Y. TIMES, June 10, 2010, at B2. Google's popular Gmail system has been successfully breached. *See* Jason Arrington, *Google Reveals Data Security Breach on Gmail*, CRYPTZONE (June 2, 2011), http://www.cryptzone.com/news/article.aspx?category=Email-security&title=Google-reveals-data-security-breach-on-Gmail&id=800565910.

253. Passed just six weeks after the September eleventh attacks, the USA PATRIOT Act was implemented in response to the national security crisis but has been criticized as being overly broad and weakening privacy protections by, in many cases, eliminating the requirement that investigators show probable cause for collecting personal information. *See, e.g.*, Derek M. Alphran, *Changing Tides: A Lesser Expectation of Privacy in a Post 9/11 World*, 13 RICH. J.L. & PUB. INT. 89 (2009) (arguing that despite the lack of recent immediate known terrorist threats, the "war on terror" has made invasions of privacy in public and private places an accepted norm); Fred H. Cate, *Government Data Mining: The Need for a Legal Framework*, 43 HARV. C.R.-C.L. L. REV. 435, 436 (2008) (asserting that claims that more government access to information could have prevented the September eleventh attacks has fueled an "apparently insatiable government appetite for access to and retention of personal data, especially from the vast databases routinely maintained by the private sector"); Kelly R. Cusick, *Thwarting Ideological Terrorism: Are We Brave Enough to Maintain Civil Liberties in the Face of Terrorist Induced Trauma*, 35 CASE W. RES. J. INT'L L. 55 (2003) (alleging that

tential future legislation will be comprehensive in the sense of addressing a wider array of information problems than current statutes, it is also likely—as in the case of legislation relating to medical information—to present fine-grained, context-dependent rules. For example, we may have the right to keep our mobile phone carriers—but not the government—from making or keeping records of our location based on the GPS capacities of our phones.[254] Again, let us for a moment assume, as we did with respect to medical information, that individuals *do* have property rights in personal information and that those rights afford them some degree of control over data pertaining to them. It does not follow that the powers that individuals gain or retain from comprehensive information-protection legislation will look like conventional property rights. Instead, the powers are likely to be significantly curtailed to accommodate other competing interests at issue. If by some chance the powers afforded to individuals do look like property rights, it will be because individual control does not threaten institutional and governmental concerns, not because "property" demands any particular solution.

C. *W(h)ither Property?*

I have suggested in this Part that the legal category "property" will not determine individuals' rights to control their medical information specifically or their personal information generally—that health- and information-specific policies will determine how many, and what kind of, powers individuals will have with respect to information. In making these suggestions, I do not mean to argue that property has altogether lost its meaning, integrity, or coherence as a legal category.[255] I mean instead to challenge the connection that is fundamental to arguments for propertization of information, the connection between property and control.

Recall that property "solves" the problem of information control by giving owners veto power over the use of their personal information. If individuals "own" their information, then they—and only they—can control

---

though the purpose of the Patriot Act was to prevent terrorism, some provisions grant overly broad surveillance powers that extend beyond preventing terrorism).

254. Apple and Google have used their products to breach customers' security. Apple used Wi-Fi access points and cell tower locations to track iPhone and iPad users' locations, storing the unencrypted information on the Apple device and users' computers upon synchronization, making the information vulnerable to hacking. *See* Miguel Helft, *Jobs Concedes Apple's Mistakes, and Promises a Fix on Location Data Practice*, N.Y. TIMES, Apr. 28, 2011, at B3; *iSpy: Your iPhone Knows Where You've Been*, CHI. TRIB., Apr. 22, 2011, at C3; David Sarno, *Apple Denies Tracking iPhones*, L.A. TIMES, April 28, 2011, at B1. Google used its Android phones to collect data on Wi-Fi hot spots, enhance its mapping features, and provide marketing based on users' locations. Miguel Helft, *Phone Data Used to Fill Digital Map*, N.Y. TIMES, Apr. 26, 2011, at B1; Yukari Iwatani Kane, *House Panel Widens Inquiry Into Tracking to More Firms*, WALL ST. J., Apr. 26, 2011, at B3.

255. *Cf.* Thomas C. Grey, *The Disintegration of Property*, *in* NOMOS XXII: PROPERTY 68, 81–82 (J. Roland Pennock & John w. Chapman eds., 1980) (arguing that property has ceased to be an important category in legal and political theory).

if and under what circumstances that information is used. But just as arguments about propertization of information make simplified assumptions about property's alienability, this argument makes simplified assumptions about the connection between ownership and control.

If all property rights were rights to exclude, then the relationship between ownership and control would be relatively uncomplicated. *In rem* exclusion rights can be understood as a sort of delegation of powers that "allows owners to undertake the choice among uses without having to justify the decision to third parties."[256] There is serious disagreement among property theorists over the question of whether exclusion is central to property law,[257] but, tellingly, there is agreement that not all property rights are rights to exclude.[258] Trespass is important to property, but so is nuisance.

In many of the arguments for propertization, the "owner" of information is depicted as exercising something very like Blackstone's infamous "despotic dominion" over what is hers.[259] She does or does not decide to keep information secret; she does or does not agree to various proposed contracts with respect to her information; she does or does not give website owners freedom to make unfettered use of whatever they glean from her activity on their sites. But putting aside the information issues that might distort these decisions, the underlying vision of ownership-as-freedom does not conform to reality. Even physical property is far less amenable to consolidated control than is sometimes thought. Most ownership rights are qualified: zoning limits the ability of fee simple owners to do whatever they want on their land; the revolution in landlord-tenant law has led to new rules that limit landlords' freedom of action with respect to leased property in numerous ways; covenants and easements impose still other restrictions on owners' ability to do whatever they might like on their own land. Where property is owned in common, co-owners owe each other a variety of duties, and control rights are shared. From environmental law to occupancy limits, federal, state, and local statutes constrain owners' powers in significant respects.

---

256. Smith, *supra* note 83, at 984; *see also* Smith, *supra* note 98, at 1728 ("Property responds to uncertainty over uses by bundling uses together and delegating to the owner the choice of how to use the asset.").

257. *See* Baron, *supra* note 85, at 919–20.

258. As noted *supra* text accompanying notes 101–105, those who put exclusion at the core of property nonetheless see a role for more complex "governance" rules. *See, e.g.*, Merrill & Smith, *supra* note 81, at 797–98; *see also* Smith, *supra* note 87, manuscript at 9 ("exclusion is not the whole story").

259. On Blackstone's infamous statement describing property as "that sole and despotic dominion which one man claims and exercises over the external things of the world, in total exclusion of the rights of any other individual in the universe," 2 WILLIAM BLACKSTONE, COMMENTARIES *2, see Carol M. Rose, *Canons of Property Talk, or, Blackstone's Anxiety*, 108 YALE L.J. 601, 602 (1998) (asserting that "Blackstone posed his definition more as a metaphor than as a literal description—and as a slightly anxiety-provoking metaphor at that").

In the eyes of some theorists, these limits are exceptional;[260] in the eyes of others, these limits are the norm.[261] Either way, property does not always or necessarily entail control. The contrary is also true, as substantial control rights can exist without ownership.[262] In the end, property is sometimes power, but not always. Within property law and theory, the extent to which ownership gives rise to any particular form of control is a matter of controversy, and today's resolution of that question may not be the same as its resolution at another time. Information doesn't tell a new story about control; it merely updates an old one.

We can call information "property" if we want to, but, as with alienability, we will still have to decide exactly how much control individuals can exert, and under precisely what circumstances. These are hard questions. The digitization of medical information, with its proliferation of potential owners and its multiplication of relationships among those owners, makes the hard question of how much control any individual can have even harder. But to answer that question we will need to do more than simply invoke the category "property." No legal category can define itself. Whether we decide to give individuals "property" rights in their personal information or not, we will have to make hard choices about how power and authority—control—will be shared in a world of increasing interconnection.

Conclusion

One explanation of why property seems such a promising avenue for control of personal information relates to the limits of language. As Julie Cohen notes, "private" means "not common-owned, and set apart from that which is common and owned by others."[263] Things that are not owned, in contrast, "are presumptively accessible to all."[264] As we have seen, what we want with respect to personal information is control. But "we lack a word for describing control over things without legal or beneficial ownership of them—a word that signifies that the thing described is both not common and not owned."[265] For lack of a word, we try another—property—because we simply can't help ourselves.

This Article has argued that however natural it may be to talk about information control in property terms, it is also misleading. Issues of whether property is centered around exclusion, involves consolidated rights, operates *in rem*, or requires standardized forms are all issues about *the extent to*

260. *See, e.g.*, Smith, *supra* note 81, at 79; Smith, *supra* note 98, at 1755–58.

261. *See, e.g.*, Singer, *supra* note 118, at 1052–53. For a summary of this debate, see Baron, *supra* note 85, at 945–52.

262. One can, for example, control the use of property one does not own through easements and servitudes.

263. Cohen, *supra* note 6, at 1379 (internal quotation marks omitted).

264. *Id.* at 1379.

265. *Id.* at 1379.

which property gives individuals control over what they own. Because the degree to which property grants control is itself fundamentally contested within property law and theory, "property" cannot tell us how much control individuals should have over their medical or personal information.

In the end, there is no consensus that the attenuated control that can realistically be asserted in the context of personal information is appropriately called "property" at all. Nor is there consensus on whether the rhetoric of property points us toward or away from the values at play when the "good" in question is some aspect of our very "selves." Finally, if there is "property" in information, it may be a very unappealing kind of property—a claim derived from envy of the value that others have found in what we had ignored or thought worthless.

Controlling information of all kinds requires hard choices. Individuals legitimately worry about what the world might come to know about them and how the world might come to know it. But individuals' concerns are but one part of a very large equation. With respect to EHRs, that equation includes, *inter alia*, considerations of health policy and public health. With respect to personal information more generally, the equation includes, *inter alia*, financial, national security, and free speech concerns. Individuals no doubt should be granted *some* power to control their personal information. But the concept of property alone cannot tell us how much, or what kind, of power. This uncertainty is not new, and it is not necessarily problematic. In a world that is ever more interconnected, power and control will inevitably be shared.