THE JOHN MARSHALL
REVIEW OF INTELLECTUAL PROPERTY LAW

THE OWNERSHIP AND EXPLOITATION OF PERSONAL IDENTITY IN THE NEW MEDIA AGE

THOMAS HEMNES

ABSTRACT

Personally Identifiable Information ("PII") has never been more valuable. In today's networked world, seemingly trivial facts can be collected, molded into a marketable economic profile, and transferred in the blink of an eye. To be sure, the commodification of PII allows for provision of dramatically more efficient and effective services. Yet the potential for privacy abuses is substantial. What interest does one have in the constellation of facts that defines one's identity? Is it something one can own, like their right of publicity? Or are others free to use what they learn about a person? This article surveys current privacy law and policy across jurisdictions with a view to providing both positive and normative answers to these increasingly important questions.

Cite as Thomas Hemnes, *The Ownership and Exploitation of Personal Identity in the New Media Age*, 12 J. MARSHALL REV. INTELL. PROP. L. 1 (2012).

THE OWNERSHIP AND EXPLOITATION OF PERSONAL IDENTITY IN THE NEW MEDIA AGE

THOMAS HEMNES

THE OWNERSHIP AND EXPLOITATION OF PERSONAL IDENTITY IN THE NEW MEDIA AGE

THOMAS HEMNES*

INTRODUCTION

The lay person thinks of property in binary terms: a thing is mine or it is not. This probably stems from a very primitive, tactile sense of possession—if it's in my hand, I've got control over the thing and I can prevent you from using it, which makes it mine.[1] Among children, disputes over ownership are resolved this way, and a tug of war resolves ownership by resolving possession. For a child, possession is ten tenths of the law.[2]

As lawyers, we are trained and accustomed to thinking of property in a somewhat more nuanced way—as a "bundle of rights."[3] A child's ownership of a baseball bat gives her the right to possess it, to autograph it, to burn it, to sell it, to play baseball with it (subject of course to the rules of the game), but not the right to hit someone with it or to smash a window with it. Ownership of real estate is even more constrained by rule, regulation and custom.[4] But the binary underpinnings remain: as to each right in the bundle, either I own it or I don't; either I have the right to exclude others from its use or I don't.[5] Some of the rights may be linked; others may be divisible, but each of them is thought of as mine or not.[6] The "bundle

---

* The author gratefully acknowledges the insights and assistance of Gina Perini, Veronica Louie, Tristan Walsh and the editorial staff of the John Marshall Review of Intellectual Property Law in the preparation of this article.

[1] *See* ROBERT P. MERGES, JUSTIFYING INTELLECTUAL PROPERTY 100 (Harvard Coll. ed., 2011) ("The very definition of a property right is a claim 'good against the world,' often described as a 'right to exclude others from the particular legal interest involved . . . ."). I recommend to the reader Robert Merges' excellent disquisition. *Id.*

[2] One easily overlooks how potent such memories and images can be in our more adult conceptions.

[3] *See* Michael A. Heller, *The Boundaries of Private Property*, 108 YALE L.J. 1163, 1192 n.150 (1999) (documenting broad use of the "bundle of rights" metaphor in U.S. cases since 1940); VAN LINDBERG, INTELLECTUAL PROPERTY AND OPEN SOURCE 17 (Andy Oram ed., 3d ed. 2008) (describing property as a collection of independent rights, which "may be individually sold, licensed, given away, or destroyed").

[4] *See* Heller, *supra* note 3, at 1173–74 (1999) (discussing the bevy of modern rules and regulations affecting real property).

[5] *See* Michael A. Carrier, *Cabining Intellectual Property Through a Property Paradigm*, 54 DUKE L.J. 1, 52 (2004) (positing that the right to exclude is the most fundamental property right).

[6] John Page, *Grazing Rights and Public Lands in New Zealand and the Western United States: A Comparative Study*, 49 NAT. RESOURCES J. 403, 404–05 (2009) ("This fragmentation allowed society to treat private property rights as severable, such that the hallmark rights . . . are distinct 'sticks.' This notion of property as a divisible and relative bundle of rights has specific resonance in relation to private rights in public land."). Of course, there is the possibility of joint ownership, where two or more persons share ownership as against the rest of the world. *See generally* United States v. Craft, 535 U.S. 274, 279–82 (2002) (describing the three principal notions of joint ownership in U.S. Law).

of rights" phrase itself calls to mind an image of a bundle of sticks held in the hand, rather like the arrows held in the claw of the American Eagle. "I've got them; they're mine; you're excluded."

We have even extended this binary conception into the realm of intellectual property,[7] which by its nature is not capable of physical possession.[8] By federal statute, and indeed by the Constitution, patents and copyrights have an owner—the inventor or author—who holds in his hand the bundle of rights defined by the statute.[9] Those rights fundamentally permit the owner to exclude use by others.[10] By common law and state statute, trade secrets are much the same: they are owned by the person to whom they provide a competitive advantage.[11] The only difference is that they can slip through the owner's fingers rather easily if they are disclosed without restriction.[12] Patents, copyrights, and trade secrets are capable of joint ownership,[13] but that only means that more than one person or entity is on one side of the binary line; the whole world is on the other side.

Trademarks are different. In the first place, they cannot be owned "in gross"—no one can control all uses of a word or symbol;[14] the rights of the owner are necessarily linked to the use to which the mark is put.[15] Furthermore, it is said that trademark law is intended to protect rights of the consumer against confusion as well as the rights of the provider against misappropriation.[16] Ultimately, trademarks are intended to function as signposts, guiding the consumer to the source of goods or services.[17] Trademark infringement is misdirection[18]—a harm to the consumer—as much as it is misappropriation[19]—a harm to the provider. The law recognizes that both consumers and producers derive value from trademarks, and therefore attempts

---

[7] LINDBERG, *supra* note 3, at 17 (applying the "bundle of rights" paradigm to intellectual property).

[8] Xuan-Thao N. Nguyen, *Holding Intellectual Property*, 39 GA. L. REV. 1155, 1185 (2005).

[9] *See* U.S. CONST. art. I, § 8, cl. 8 (guaranteeing authors and inventors exclusive rights to their writings and discoveries); 35 U.S.C. § 261 (2012); 17 U.S.C. § 201; Beech Aircraft Corp. v. EDO Corp., 990 F.2d 1237, 1248 (Fed. Cir. 1993) (stating patent rights initially vest in the inventor).

[10] 17 U.S.C. § 106; 35 U.S.C. § 271.

[11] RESTATEMENT (FIRST) OF TORTS § 757 (1939) ("A trade secret may consist of any formula, pattern, device or compilation of information which is used in one's business, and which gives him an opportunity to obtain an advantage over his competitors who do not know or use it.").

[12] *See* Ruckelshaus v. Monsanto Co., 467 U.S. 986, 1002 (1984) (stating that one may extinguish one's right to a trade secret either by publicly disclosing it or by failing to take reasonable measures to maintain its secrecy).

[13] 17 U.S.C. § 201(a) (providing that authors of "a joint work are co-owners of copyright in the work"); 35 U.S.C. § 116 ("When an invention is made by two or more persons jointly, they shall apply for patent jointly . . . .").

[14] JONATHAN D. ROBBINS, ADVISING EBUSINESSES § 2:40 (2012).

[15] *See* Time, Inc. v. Petersen Publ'g Co., 173 F.3d 113, 118 (2d Cir. 1999); 15 U.S.C. § 1125 (2012). Where rights are defined by registration, the registration will be limited to defined uses or classes and the rights are subject to forfeiture if not actually used within a period of time following registration. *Id.* § 1127.

[16] 1 J. THOMAS MCCARTHY, MCCARTHY ON TRADEMARKS AND UNFAIR COMPETITION § 2:2 (4th ed. 2012); *see also* Two Pesos, Inc. v. Taco Cabana, Inc., 505 U.S. 763, 781–82 (1992) (explaining trademarks have a dual purpose to protect consumers and legitimate business interests).

[17] *See* 1 MCCARTHY, *supra* note 16, § 2:2.

[18] *Id.* § 2:33.

[19] *Id.* § 2:30.

to balance the interests of both constituencies.[20] If one defines property as a bundle of rights, each of which is capable of ownership as against the world,[21] one might even question whether trademarks should be considered a species of property at all[22]—quite ironically, because in many cases (Coca Cola, McDonald's, Levi's) they might be considered the most valuable assets of their putative owners.[23]

I begin with the question: can we understand personally identifiable information ("PII")[24] as property in this context? Does it fall within the binary ownership framework we apply to patents, copyrights and trade secrets,[25] or is PII more akin to trademarks, where rights are in some sense shared between the original creator and the world at large?[26] There is no doubt that PII has high value, particularly as it flows through the channels of electronic commerce, and most particularly as it is pooled into what is dubbed Big Data.[27] Ironically, though, we will see that it attains and holds this value without having become property in any traditional sense of the word. We will also see that when it is collected to form an

---

[20] *Id.* § 2:33

[21] *Id.* § 2:14

[22] *See* Kenneth L. Port, *The Congressional Expansion of American Trademark Law: A Civil Law System in the Making*, 35 WAKE FOREST L. REV. 827, 834 (2000) (claiming it is more convincing to speak of trademarks as property in civil law jurisdictions than in the United States).

[23] *See* Jacob Siegel Co. v. Fed. Trade Comm'n, 327 U.S. 608, 612 (1946) (stating that trade names are valuable corporate assets).

[24] PII is defined variously by the plethora of laws and regulations addressing it. The EU Data Protection Directive, Directive 95/46, of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) 31 (EC), defines "personal data" as "any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity. *Id.* art. 2(a). For purposes of U.S. government agencies, the U.S. Department of Commerce has published Guide that defines personally identifiable information as "any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information." ERIKA MCCALLISTER ET AL., U.S. DEP'T OF COMMERCE, GUIDE TO PROTECTING THE CONFIDENTIALITY OF PERSONALLY IDENTIFIABLE INFORMATION (PII) (2010).*; see also Personally Identifiable Information (PII)*, U.S. GEN. SERVICES ADMIN., http://www.gsa.gov/portal/content/104256 (last visited Oct. 14, 2012) (defining personally identifiable information as "information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual").

[25] *See* Carrier, *supra* note 5, at 53 (claiming the bundle of rights theory is predominate).

[26] *See, e.g.*, *Who, What, Why: In Which Countries Is Coca-Cola Not Sold?*, BBC NEWS MAG. (Sept. 11, 2012, 5:48 PM), http://www.bbc.co.uk/news/magazine-19550067?print=true (describing the relationship between Coca-Cola and consumers in light of the worldwide recognition of the Coca-Cola mark).

[27] *See* ANN CAVOUKIAN & JEFF JONAS, INFO. & PRIVACY COMM'R OF ONT., CAN., PRIVACY BY DESIGN IN THE AGE OF BIG DATA 3 (June 8, 2012), http://privacybydesign.ca/content/uploads/2012/06/pbd-big_data.pdf (warning of the potential for misuse of personally identifiable information compiled in "big data" systems).

image of a person it is not owned by that person at all. In other words, the playground paradigm for property ownership founders in the realm of New Media.[28]

I. THE ELEMENTS OF VALUE

One might think of these issues by analogy to a watershed. The vast aggregations of information that flow through the Internet, the value of which is pooled and captured along the way in servers and databases that throw off value like hydroelectric stations, all begin with tiny droplets of information generated by individuals and their individual transactions. It is worth asking, as to each of these droplets, what bundle of rights attach to it, and whether anyone "owns" the individual elements of that bundle.

A. Basic Facts about Individuals

One begins with information that defines who an individual is: name, sex, address, social security number, date of birth, place of birth, citizenship, telephone number, and facial and characteristics of appearance.[29] Who owns this information? It would be tempting to say that this information is owned by the particular individual to which it relates. Such a conception would fit neatly into an intellectual property scheme in which an original owner licenses or assigns rights to the next person in the "chain of title" who then licenses or assigns the information downstream into the large, valuable pools of data that can be exploited for value.[30] Reinforcing this conception, companies such as Facebook purport to acknowledge that their users "own" the personal information they provide.[31] This, however, is not the case. One searches the laws of the United States[32] or Europe[33] in vain for any

---

[28] *See Definition of: New Media*, PCMAG.COM, http://www.pcmag.com/encyclopedia_term/0,2542,t=new+media&i=47936,00.asp (last visited Sept. 16, 2012) *(*defining new media as "forms of communicating in the digital world, which includes publishing on CDs, DVDs and, most significantly, over the Internet[,]" and as "[t]he concept that new methods of communicating in the digital world allow smaller groups of people to congregate online and share, sell and swap goods and information").

[29] *See supra* note 24 and accompanying text. Information of this kind is regulated as "personal information" or "personal data" under the data protection laws of most major jurisdictions. *Id.*; *see also, e.g.*, 201 MASS. CODE REGS. 17.02 (2012); CAL. CIV. CODE § 1798.80(e) (West 2012).

[30] Patricia Mell, *Seeking Shade in a Land of Perpetual Sunlight: Privacy as Property in the Electronic Wilderness*, 11 BERKELEY TECH. L.J. 1, 71 (1996); *see also* Vera Bergelson, *It's Personal but Is It Mine? Toward Property Rights in Personal Information*, 37 U.C. DAVIS L. REV. 379, 412 (2003) (noting that the value in something like an individual's name comes from a third party collecting and organizing that name among a list of others).

[31] *See Information We Receive About You*, FACEBOOK, https://www.facebook.com/about/privacy/your-info#usernames (last visited Oct. 14, 2012) ("While you are allowing us to use the information we receive about you, you always own all of your information.").

[32] *See, e.g.*, 5 U.S.C. § 552a (2012) (providing an example of a United States law regarding the sensitivity of one's personal information, but not providing for private ownership over that information). The Privacy Act of 1974 was a very early federal regulation respecting personal

statute or principle respecting personal identity that is analogous to § 201(a) of the Copyright Act—"Copyright . . . vests initially in the author . . . ."[34]—or § 261 of the Patent Act—"[P]atents shall have the attributes of personal property."[35] Nothing in the law says that you own the fact that you are yourself—your identity.[36]

The European Personal Data Protection Directive[37] ("EU Directive") is instructive in this regard. Article 7 provides that personally identifiable data may be "processed"[38] only when one of the following circumstances obtains:

- the data subject has given his consent
- the processing is necessary for the performance of or the entering into a contract
- processing is necessary for compliance with a legal obligation
- processing is necessary in order to protect the vital interests of the data subject
- processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed
- processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the

---

information. *Id.* It applies only to federal agencies, requiring them to give notice when they collect personal information, to give individuals access to personal information collected by agencies, and a right to correct such information when it is incorrect. *Id.; see also* E-Government Act of 2002, Pub. L. No. 107-347, 116 Stat. 2899 (requiring, among other things, federal agencies to develop Privacy Impact Assessments regarding their collection and retention of personal information).

[33] This paper will be largely limited to U.S. and U.K./EU law, although the laws of most developed countries are analogous.

[34] 17 U.S.C. § 201.

[35] 35 U.S.C. § 261.

[36] *See* Mell, *supra* note 30, at 26–41. Patricia Mell acknowledges this fact, but argues that the law must extend the concept of property to encompass identity in the form of an electronic persona or personae. *Id.* In her view, the "fee simple" in each collection of electronic facts comprising an image of a person—a persona—should be owned by the individual, forcing others with an interest in those facts, the government, the public, commercial institutions to bargain with the individual for rights of use. *Id.* This is a sweeping and bold assertion, highly protective of the individual, but one that has not gained traction in the sixteen years since her publication. Identity, however, by its nature, cannot enjoy the exclusionary rights associated with all forms of property.

[37] Directive 95/46, of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) 31 (EC) [hereinafter EU Directive]. The European Commission recently proposed amendments to the Directive. *Commission Proposes a Comprehensive Reform of Data Protection Rules to Increase Users' Control of Their Data and to Cut Costs for Businesses,* EUROPA PRESS RELEASES RAPID (Jan. 25, 2012), http://europa.eu/rapid/pressReleasesAction.do?reference=IP/12/46&format=HTML&aged=0&langua. ge=en&guiLanguage=en. The proposed amendments are controversial in several respects, and have been criticized by the United States Department of Commerce. *See* DEP'T OF COMMERCE, INFORMAL COMMENT ON THE DRAFT GENERAL DATA PROTECTION REGULATION AND DRAFT DIRECTIVE ON DATA PROTECTION IN LAW ENFORCEMENT INVESTIGATIONS 1 (2012).

[38] EU Directive, *supra* note 37, art. 2(b). For purposes of the EU Directive, "processing" includes "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.*

> data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject[39]

What is noteworthy for our purposes is that, under the EU Directive, "processing" personal data, which includes collecting, using and disclosing, is generally permitted as long as the purpose is "legitimate" and does not violate "fundamental rights and freedoms."[40] The individual *can* give her consent, but it is not *required*.[41] The person collecting and using the personal data, even in the EU, does not need the individual's consent to do so.[42]

An individual thus has no general right to exclude others from knowing basic elements of her personal identity.[43] She does, however, have some control over these basic elements of personal identity. She can change her address or telephone number,[44] with a bit more difficulty change her name,[45] and with considerably more difficulty change her citizenship or social security number.[46] But it is very difficult to change one's facial appearance[47] and literally impossible to change one's date and place of birth or age,[48] however much one might want to do so. Under Article 12 of the EU Directive, the data subject also has the right to access all data processed about her and the right to demand the rectification, deletion, or blocking of data that is incomplete, inaccurate, or is not being processed in compliance with the data protection rules.[49] With considerable variation, depending on the jurisdiction of residence, she can also have certain elements of this information—notably a telephone number[50] or a social security number[51]—withheld from the public at large.

---

[39] *Id*. art. 7.

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

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

[42] *Id*. art. 7 (providing disjunctive conditions for making data processing legitimate).

[43] *See id*.

[44] *See, e.g.*, *Change of Address—Online Forms*, USA.GOV, http://www.usa.gov/Citizen/Services/Change-Of-Address.shtml (last visited Oct. 16, 2012); *Change Your Phone Number on Sprint.com*, SPRINT, http://support.sprint.com/support/article/Change_your_phone_number_on_sprintcom/case-ib376964-20090701-102238?INTNAV=SU:AL:MVT (last visited Oct. 16, 2012).

[45] *See, e.g.*, 735 ILL. COMP. STAT. 5/21-101 (2007).

[46] *See, e.g.*, *N-400 Application for Naturalization*, U.S. CITIZENSHIP AND IMMIGR. SERVICES, http://www.uscis.gov/portal/site/uscis/menuitem.5af9bb95919f35e66f614176543f6d1a/?vgnextoid=480ccac09aa5d010VgnVCM10000048f3d6a1RCRD&vgnextchannel=40a9b2149e7df110VgnVCM1000004718190aRCRD (last updated Apr. 6, 2012); *Identity Theft and Your Social Security Number*, U.S. SOC. SECURITY ADMIN. (Oct. 2012), http://www.socialsecurity.gov/pubs/10064.html#a0=5&new= (follow "Should you get a new Social Security number" hyperlink) (explaining the conditions and requirements for obtaining a new Social Security Number).

[47] *See Clinical Policy Bulletin: Face Transplantation,* AETNA, http://www.aetna.com/cpb/medical/data/800_899/0819.html (last modified Sept. 2, 2011).

[48] *See, e.g.*, *Corrections to Birth Records,* ILL. DEP'T OF PUB. HEALTH, http://www.idph.state.il.us/vitalrecords/correctioninfo.htm (last visited Sept. 29, 2012) (explaining that amendments to birth records are only permissible to correct mistakes).

[49] EU Directive, *supra* note 37, art. 12. This principle has no general application under United States law, but some specific manifestations in places such as the Fair Credit Reporting Act. *See* 15 U.S.C. §§ 1681–1681x (2012).

[50] *See* 47 C.F.R. § 51.217(c)(iv) (2012) ("A [local exchange carrier] shall not provide access to unlisted telephone numbers, or other information that its customer has asked the LEC not to make available, with the exception of customer name and address . . . .").

Furthermore, she can prevent others from pretending to be her.[52] But at the base, she cannot prevent third parties from possessing and using the most fundamental pieces of information about her: those pieces that define who she is, at least for the purpose of identifying her.[53] That is, one might say, information that the individual does not own, any more than one owns one's personal appearance. One can marginally influence it and mold it, but in the end, it is others who see it and identify us by it. And they have a perfect right to do that; if people had no right to identify one another, all commerce—indeed all human interaction—would be impossible. You have to know with whom you are dealing.[54]

Basic information about individuals has some value in the marketplace.[55] Facebook recently acquired Face.com,[56] creators of a facial recognition software product, suggesting that Facebook sees value in the ability to recognize individuals by their appearance.[57] My age, my sex, where I live, my telephone number, what I do for a living—all of these narrow somewhat the goods or services I might be interested in buying, and at least permit a merchant to avoid wasting money trying to sell me things I am highly unlikely to buy.[58] But when combined with other facts about me, as well as my purchasing and lifestyle habits, the information can become considerably more valuable and also considerably more subject to potential abuse.[59] We now turn to these other bits of information.

B. Sensitive Facts about Individuals

The EU Directive, implementing legislation in the member states, and United States state and federal law, all identify categories of information about the individual that are considered particularly sensitive and subject to special

---

[51] In many jurisdictions, publishing of social security numbers is prohibited. *See, e.g.*, MICH. COMP. LAWS §§ 445.81–.87 (2012)*;* ARIZ. REV. STAT. ANN. § 44-1373 (2012).

[52] Identity Theft and Assumption Deterrence Act of 1998, 18 U.S.C. §§ 1001, 1028. A closely analogous concept is the right of a celebrity to control use of his or her identity for personal gain (the "right of publicity"). *See, e.g.*, CAL. CIV. CODE § 3344 (West 2012).

[53] *See, e.g.*, CAL. CIV. CODE § 1798.83(d)(1)(A); EU Directive, *supra* note 37, art.2(b).

[54] *See* 18 U.S.C. § 1028. Here again the analogy to trademarks is instructive. Trademark law protects the interest of the public in knowing the source or origin of goods and services. 15 U.S.C. § 1127. Identity law, if we may call it that, protects the interest of everyone in knowing whom they are dealing with. *See* 18 U.S.C. § 1028.

[55] 2 MCCARTHY, *supra* note 16, § 11:32 ("Even for noncelebrities, there exists a marketplace for the use of the identity of ordinary people in advertising.").

[56] Lauren Indivik, *Facebook Acquires Face.com*, MASHABLE BUS. (June 18, 2012), http://mashable.com/2012/06/18/facebook-acquires-face-com/.

[57] Samantha Murphy, *Facebook's Facial-Recognition Acquisition Raises Privacy Concerns*, MASHABLE SOC. MEDIA (June 25, 2012), http://mashable.com/2012/06/25/facebook-facial-recognition-privac/.

[58] *See* FED. TRADE COMM'N, FTC STAFF REPORT: SELF-REGULATORY PRINCIPLES FOR ONLINE BEHAVIORAL ADVERTISING, at i (2009), *available at*, http://www.ftc.gov/os/2009/02/P085400behavadreport.pdf (citing benefits of behavioral advertising).

[59] *See* Jacobs v. Nat'l Drug Intelligence Ctr., 423 F.3d 512, 518 (5th Cir. 2005) (explaining that the primary purpose of 5 U.S.C. § 522a(b) is to prevent publicizing information that is detrimental to a person's character or reputation).

protections.[60] While the exact types of information that are considered sensitive vary from jurisdiction to jurisdiction,[61] there is an international consensus that two categories of information—information that could be used for purposes of unlawful discrimination and financial information—deserve special attention and protection.[62]

1. Information subject to potential abuse

Information in the category of being subject to potential abuse always includes information about an individual's health, which is universally considered sensitive and subject to special protection.[63] It may also include information about religion, political affiliation, marital status, and sexual orientation, among other categories.[64] Article 8 of the EU Directive defines this as "data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life."[65] The United Kingdom implementing legislation, the U.K. Data Protection Act of 1998,[66] expands this definition slightly, defining "sensitive personal data" as data about the individual's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition, sexual life, or criminal history.[67] A number of states in the U.S. have adopted legislation that similarly regulates "sensitive personal information," typically protecting information relating to an

---

[60] *See* EU Directive, *supra* note 37, art. 8 (prohibiting the use of "data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, . . . and health or sex life"); Data Protection Act, 1998, c. 29, § 2 (Eng.) [hereinafter Data Protection Act] (implementing the EU Directive and further protecting personal data regarding the commission of a crime or related proceedings); 815 ILL. COMP. STAT. § 530/5 (2012) (restricting the collection of personal information including an individual's first and last name in conjunction with Social Security number, driver's license number, state identification card number, or financial account information, such as bank or credit card number, access code, and password); 42 U.S.C. § 1320d–6(a) (2012) (protecting individually identifiable health information); 5 U.S.C. § 552a(a)(4) (defining records about individuals that government agencies may not disclose).

[61] *Compare* EU Directive, *supra* note 37, art. 8. (deeming information about racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and health or sex life sensitive information), *and* Data Protection Act, *supra* note 60, § 2 (deeming the same in addition to criminal history), *with* 815 ILL. COMP. STAT. § 530/5 (prohibiting the collection of first and last names in conjunction with a Social Security number, driver's license or state identification number, or financial account number), *and* 5 U.S.C. § 552a (prohibiting government agencies from disclosing information about citizens related to "education, financial transactions, medical history, and criminal or employment history and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph").

[62] *See, e.g.*, EU Directive, *supra* note 37, art. 8 (defining sensitive personal data); Title VII of the Civil Rights Act of 1964 § 703(a), 42 U.S.C. § 2000e-2(a) (making it unlawful for employers to discriminate based on "race, color, religion, sex, or national origin"); 815 ILL. COMP. STAT. § 530/5 (protecting personal financial information).

[63] *See, e.g.*, 42 U.S.C. § 17935.

[64] *See* Data Protection Act, *supra* note 60, § 2.

[65] EU Directive, *supra* note 37, art. 8.

[66] Data Protection Act, *supra* note 60.

[67] *Id.* § 2.

individual's physical or mental health.[68] At the U.S. federal level there is no general regulation of sensitive personal information falling into this category, but the Health Insurance Portability and Accountability Act ("HIPAA")[69] provides a broad definition of health-related information that is subject to strict standards regarding safety and disclosure.[70]

Article 8 of the EU Directive requires member states to prohibit entirely the "processing" of any such sensitive personal information, unless the processing is for one of a limited set of permitted purposes.[71] This brings sensitive personal data closer to the exclusionary right of a property owner, but not the whole way.[72] Although the purposes for which sensitive personal data may be processed without the individual's consent are substantially narrower than those applicable to personal information generally,[73] they are broad enough that it would be difficult to say that an individual owns his sensitive personal data.[74] As an example, the permissible purposes for which basic personal information may be processed include "performance of a contract."[75] This is not a permissible purpose with respect to sensitive personal data, but meeting one's obligations under employment law is a permissible purpose for processing sensitive personal data.[76] It is also permissible to process personal data for purposes of delivering health services.[77]

United States law regarding sensitive personal information is fundamentally different.[78] There is no general prohibition on its collection or dissemination;[79] instead, laws tend to focus on the misuse of such information for discriminatory purposes.[80] Thus, it is quite legal in the U.S. to maintain and sell a database listing Democrats or Republicans or Mormons or Native Americans.[81] There is not even a hint in our law that such information is private or belongs to the individual.[82] On the

---

[68] *See, e.g.*, TEX. BUS. & COM. CODE ANN. § 521.002(a)(2)(B) (West 2012).

[69] Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936.

[70] Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, sec. 262, §§ 1171–77, 110 Stat. 1936, 2021–29 (codified as amended at 42 U.S.C. §§ 1320d–1320d-6 (2012)).

[71] EU Directive, *supra* note 37, art. 8.

[72] *Compare* Data Protection Act, *supra* note 60, § 10 (allowing individuals to preclude others from obtaining, recording, holding, or operating on personal data, subject to a few exceptions), *with* 35 U.S.C. § 154(a)(1) (2012) (granting patent owners the unqualified right to exclude all others from "making, using, offering for sale, or selling the invention").

[73] *See* EU Directive, *supra* note 37, art. 8.

[74] *See id.* art. 7 (giving reasons why processing of personal data may be necessary even without the consent of the data subject).

[75] *Id.* art. 7(b).

[76] Data Protection Act, *supra* note 60, § 7.

[77] *Id.* § 41C.

[78] *See* 5 U.S.C. § 552a(b) (2012); 18 U.S.C. § 1028.

[79] *See* 5 U.S.C. §§ 552a(a)(7), (b); 18 U.S.C. § 1028(a).

[80] *See* 5 U.S.C. § 552a(f); 18 U.S.C. § 1028(a).

[81] *See* 5 U.S.C. §§ 552a(a)(7), (b).

[82] *See* Louis D. Brandeis & Samuel D. Warren, *The Right to Privacy*, 4 HARV. L. REV. 193, 216–17 (1890). In a back-handed way, United States law does recognize that some facts ought not to be collected and released, but the focus there is more typically on the means for capturing the information—"invasion" of privacy—than on the nature of the facts themselves. *Id.* In the United States, if a person posts embarrassing photos or videos on the Internet, he cannot complain about

other hand, if one used such a database as a criterion for hiring or firing, one could violate a wide variety of anti-discrimination laws.[83] Health information is an exception "Protected Health Information" is regulated in a manner that is more closely analogous to the European model: HIPAA features enhanced notice requirements, as well as the requirement that "Covered Entities" (generally, health care providers and insurers) obtain consent before using or disclosing protected health information for any purpose other than treatment, payment, or other health care operations.[84]

In either case, a fundamental part of the rationale for these controls is that sensitive personal information is easily subject to abuse or misuse, both by governments and by private employers, neighbors, or others.[85] Thus, the United States and the EU share a similar goal in regulating this type of information, but the means they employ to reach that end are quite different. The EU focuses on both the collection and use of such data;[86] the U.S. focuses on its misuse.[87]

2. Financial Information

The second broad category of information singled out for special protection is financial information.[88] Here, United States and European law are more closely allied.[89] For example, financial information does not fall within the United Kingdom's definition of sensitive personal information,[90] and the processing of financial information is therefore not subject to the special limitations that apply to the processing of sensitive personal information.[91] At the same time, analogues to the general EU Directive principles appear in the Fair Credit Reporting Act ("FRCA"),[92] the Gramm-Leach-Bliley Act ("GLB"),[93] and in a variety of state laws designed to protect financial information and provide a remedy if it is improperly

---

somebody else collecting and storing the information they contain. In Europe, this would be illegal if the data controller's use of the information did not fall into a narrow set of exceptions. *See* EU Directive, *supra* note 37, art. 7.

[83] *See* 42 U.S.C. § 2000e-2(a) (2012) (prohibiting employers from discriminating on the basis of "race, color, religion, sex, or national origin"); 42 U.S.C. § 12112(a) (prohibiting employment discrimination based on disabilities).

[84] *See* 45 C.F.R. § 164.508. -6.

[85] *See* Jacobs v. Nat'l Drug Intelligence Ctr., 423 F.3d 512, 518 (5th Cir. 2005) (stating that the primary purpose of 5 U.S.C. § 522a(b) is to prevent unauthorized publication of information that is detrimental to character reputation).

[86] EU Directive, *supra* note 37, art. 7; *see also* Data Protection Act, *supra* note 60 ("An Act to make new provision for the regulation of the processing of information relating to individuals, including the obtaining, holding, use or disclosure of such information.").

[87] *See* 5 U.S.C. § 552a(b); 18 U.S.C. § 1028.

[88] 15 U.S.C. § 6801 (2012).

[89] *See* Virginia Boyd, *Financial Privacy in the United States and the European Union: A Path to Translating Regulatory Harmonization*, 24 BERKELEY J. INT'L L. 939, 968–69 (2006).

[90] Data Protection Act, *supra* note 60, § 2.

[91] *Id.* § 7.

[92] Fair Credit Reporting Act, 15 U.S.C. §§ 1681–1681x.

[93] Gramm-Leach-Bliley Act, Pub. L. No. 106-102, 113 Stat. 1338 (1999) (codified as amended in scattered sections of 12, 15 U.S.C.).

disclosed.[94] FCRA permits an individual to gain access to information about his credit record and to insist on correction of erroneous information.[95] GLB requires financial institutions to adopt policies informing consumers of their policies respecting the consumers' financial information that the institution collects, protects, and uses.[96] It also gives consumers a right to opt out of information sharing beyond the collecting institution.[97] In these respects both FCRA and GLB effectively incorporate, with respect to credit and financial information, principles that are given much more general application under the EU Directive,[98] with one important difference: GLB gives only an opt-out right, whereas the EU Directive, and implementing legislation in member states, generally requires opt-in before personal information can be disseminated outside of the information controller and processers providing services to the controller.[99]

C. Behavioral Facts about Individuals

Thus far, we have discussed what one might consider comparatively static elements of personal identity. There is, however, a far more dynamic category of personal information that may have less potential for abuse than the static categories, but far more potential for commercial exploitation, particularly when it is combined with basic elements of personal identity. This category comprises the transactions and other electronic behaviors that are effected, recorded, confirmed, or stored electronically, often via the Internet.[100]

---

[94] *See, e.g.*, 201 MASS. CODE REGS. 17.01 (2012) (governing the security of, among other things, financial information). Similar laws exist in many other jurisdictions, in some cases mandating security measures and in other cases mandating disclosure and remediation following an unauthorized breach of security. *See* 15 U.S.C. §§ 6801, 6803, 1681g(d).

[95] 15 U.S.C. §§ 1681g, 1681i. In this respect, the FCRA implements one of the basic principles of the EU Directive, but only with respect to the very narrow category of credit information. *See* 15 U.S.C. §§ 1681g, 1681i.

[96] Gramm-Leach-Bliley Act, Pub. L. No. 106-102, §§ 501, 503, 113 Stat. 1338, 1436–37, 1439 (1999) (codified as amended at 15 U.S.C. §§ 6801, 6803 (2012)).

[97] *Id.* § 502, 113 Stat. at 1437–39 (codified as amended at 15 U.S.C. § 6802).

[98] *Compare* EU Directive, *supra* note 37, art. 6 (requiring Member States to provide adequate safeguards for all personal data), *and* EU Directive, *supra* note 37, art. 12 (guaranteeing individual's the right to obtain and challenge all personal data relating to the individual), *with* 15 U.S.C. § 6803 (requiring financial institutions to implement and disclose privacy policies), *and* 15 U.S.C. §§ 1681g, 1681i (permitting individual's to gain access to financial and credit information, and to challenge erroneous information).

[99] EU Directive, *supra* note 37, art. 7.

[100] *See* Steven C. Bennett, *Regulating Online Behavioral Advertising*, 44 J. MARSHALL L. REV. 899, 908–09 (2011) (discussing efforts on the part of various agencies to regulate online behavioral advertising). "Behavioral advertising," which targets individuals based on their browsing and transactional behavior, has spawned a growing legal literature. *See, e.g.*, Dustin D. Berger, *Balancing Consumer Privacy with Behavioral Targeting*, 27 SANTA CLARA COMPUTER & HIGH TECH. L.J. 3, 41–43 (2011) (discussing FTC self-regulatory principles regarding behavioral targeting in advertising); Matthew S. Kirsch, *Do-Not-Track: Revising the EU's Data Protection Framework to Require Meaningful Consent for Behavioral Advertising*, 18 RICH. J.L. & TECH. 2, 24–38 (2011) (giving an overview of the EU's Data Protection Initiative and its impact on behavioral targeting).

Information cascades from every transaction on the Internet, rushing effortlessly over international boundaries and transactions. Take this personal account as an example: My wife and I sent our daughter a Mother's Day present, a basket of fruit. To do this we logged onto the Web from where we were at the time—England—and searched Google for companies delivering fruit. We visited two different websites for fruit delivery. After scrolling through their respective offerings, we decided on a fruit basket from Edible Arrangements and ordered it to be delivered on Mother's Day to our daughter, paying with a credit card via PayPal. We promptly received an email confirmation of our order, including not only our email address, but also our daughter's address and what we sent her as well.

By then we had left a sizeable trail of valuable information that was originated in England, ran through the servers of British Telecom, then through the servers of Google/U.K., then to the servers of the ISP providers to Edible Arrangements and Edible Bouquets, and finally to the databases of Edible Arrangements and Edible Bouquets. [101] The information included PII about us: our name and address, the fact that we travel, the fact that we have a daughter, our means of payment, and even the different options we considered before landing on our selection of Mother's Day present. If we had used a mobile device, we also would have transmitted real-time information about our whereabouts, our peripatetic habits, and even our in-person shopping habits that made no use of the Internet whatsoever.[102] Like Hansel and Gretel, mobile devices leave a trail of locational breadcrumbs behind their users.[103] These crumbs are eagerly snatched by the device and service providers, who can associate them with mapping information to provide real-time advertisements and information to their users.[104] We also left a deposit of valuable information about our daughter: her name and address and the fact that she is a mother, both of which suggest targeted marketing and sales efforts that would be impossible without access to such information.

There is no doubt that companies assiduously track behavioral information. "Real-time ad bidding"—associating on-line advertisements with browsing history—is fundamental to the business models of companies such as Google and Amazon,[105]

---

[101] *See Fact Sheet 18: Online Privacy: Using the Internet Safely*, PRIVACY RTS. CLEARINGHOUSE, https://www.privacyrights.org/fs/fs18-cyb.htm#Internet_Service (last updated Oct. 2012).

[102] Melissa Loudon, *Mobile Surveillance—A Primer*, MOBILEACTIVE.ORG (June 10, 2009), http://mobileactive.org/howtos/mobile-surveillance-primer.

[103] *Id.*

[104] *See* Quentin Hardy, *Head to Head Over Mobile Maps*, N.Y. TIMES, June 18, 2012, at B1. Service and device providers such as Google and Apple compete aggressively to capture the value of mapping and location information. *See id.*; Danielle Kucera, *Apple to Feature Yelp Check-Ins Within IPhone Maps App*, BLOOMBERG (June 25, 2012), http://www.bloomberg.com/news/2012-06-25/apple-to-feature-yelp-check-ins-within-iphone-maps-app.html; Steven Duque, *Twitter Places: To Check-in or Not to Check-in?*, WALL ST. CHEAT SHEET (June 19, 2010), http://wallstcheatsheet.com/breaking-news/twitter-places-to-check-in-or-not-to-check-in.html/ (providing insight into the economic potential and social costs of location-driven services such as Foursquare and Twitter Places).

[105] Eric Savitz, *Facebook Exchange and the Rise of Real-Time Ad Bidding,* FORBES (June 14, 2012, 4:26 PM), http://www.forbes.com/sites/ciocentral/2012/06/14/facebook-exchange-and-the-rise-of-real-time-ad-bidding/print/.

and Facebook recently announced a service it calls "Facebook Exchange" that uses cookies Facebook places on browsers to target ads to Facebook users.[106] A recent study concluded that, since November 2010, behavioral tracking has increased 400%.[107] The study found that on average a visit to a website triggers fifty-six (!) instances of data collection.[108]

Who owns this information? In the U.S., end customer lists are considered a classic example of a trade secret,[109] and there is very little doubt that the customer lists of the Edible Arrangements company, and of the franchisee we chose to make and deliver the fruit, would be considered trade secrets that are owned by those companies.[110] There is also very little doubt that any additional information they can glean from my Web visit—what options I considered, how long I was on the site, how I paid, to whom the fruit was delivered, where I was when I placed the order—would be included in the information that they could protect as their trade secrets.[111] On the other hand, these facts are not quite theirs: I am perfectly free to disclose this information, and I just did. It is the aggregation of information about customers that U.S. law would protect against unauthorized disclosure (more on this later).[112] In the U.S., Edible Arrangements and its franchisee are generally free to store and use the information about my transaction, and to make money by selling it to third parties.[113]

Also, on the U.S. end, PayPal would be considered a financial institution for purposes of GLB, and their possession of my credit card and other financial information would be governed by the GLB principles.[114] They must have a privacy

---

[106] Douglas MacMillan & Jonathan Erlichman, *Facebook to Debut Real-Time Bidding for Advertising,* BLOOMBERG, (June 14, 2012), http://www.bloomberg.com/news/2012-06-13/facebook-to-debut-real-time-bidding-for-advertising.html. A Facebook user cannot opt-out of the cookies Facebook uses for this purpose. *Id.* The only way to avoid the collection and use of this data is to disable the cookies on third-party websites or on the user's browser, either of which would substantially degrade the browsing experience by requiring the user to re-input basic information every time a page is visited. *Id.*

[107] Elinor Mills, *Behavioral Data Tracking Rising Dramatically (Q&A),* CNET NEWS, (June 19, 2012, 11:55 AM), http://news.cnet.com/8301-1009_3-57456273-83/behavioral-data-tracking-rising-dramatically-q-a/.

[108] *Id.*; *see also* Bethany Rubin Henderson, *Hey That's Personal! When Companies Sell Customer Information Gathered Through the Internet*, 14 BUS. L. TODAY 13, 13 (2004) (claiming the majority of companies collect "personally identifiable information from online visitors").

[109] Kewanee Oil Co. v. Bicron Corp., 416 U.S. 470, 474–75 (1974); *see also* 18 U.S.C. § 1839 (2012) (including a compilation as a type of protectable trade secret); CAL. CIV. CODE § 3426.1(d) (2012) (defining a trade secret as any information having economic value derived from its secrecy). California is one of forty-seven states to have adopted the Uniform Trade Secrets Act definition of trade secrets. CAL. CIV. CODE § 3426.1(d).

[110] *See Kewanee Oil*, 416 U.S. at 474–75.

[111] Julie A. Katz, *To Be a Trade Secret or Not To Be a Trade Secret: Practical Considerations when Protecting IP Assets*, *in* IP VALUE 2012: BUILDING AND ENFORCING INTELLECTUAL PROPERTY VALUE: AN INTERNATIONAL GUIDE FOR THE BOARDROOM 53, 53 (10th ed. 2012), *available at* http://www.iam-magazine.com/issues/complete.ashx?g=a4169eff-870c-4f39-ad00-459d81e88bff.

[112] Hamilton-Ryker Grp., LLC v. Keymon, No. W2008-00936-COA-R3-CV, 2010 WL 323057, at *15–16 (Tenn. Ct. App. Jan. 28, 2010).

[113] 15 U.S.C. § 6802. There is in fact a very robust market in the U.S. for customer information of this kind.

[114] 15 U.S.C. § 6809(3)(A). The GLB defines "financial institution," by reference to 12 U.S.C. § 1843(k), to mean any institution in the business of engaging in activity that is (A) "financial in

policy that I have been made aware of, and must give me an opt-out right before they can sell information about me to third parties.[115] Not surprisingly, PayPal has all of these in place;[116] they have clearly given some attention to the rules and regulations in this regard. Among other things, their policy gives information about the "cookies" they leave on my computer when I do business with them,[117] which of course is another species of personal information that my transaction generated.

The Electronic Communications Privacy Act[118] makes it a crime to intercept my electronic communications while in transit,[119] and the Stored Communications Act[120] makes it a crime to access, without authorization, the Internet systems through which my wife and I placed our order.[121] The United States does not otherwise significantly regulate the collection and retention of information about my transactions, but it does impose some regulations on what can be done with the information.[122] Under the CAN-SPAM Act of 2003,[123] on-line advertisers must provide an option by which the recipient can opt-out of receiving future email advertisements.[124] Under the Telephone Consumer Protection Act of 1991,[125] a U.S.

---

nature or incidental to such financial activity" or (B) "complementary to a financial activity and does not pose a substantial risk to the safety or soundness of depository institutions or the financial system generally." *Id.*; 12 U.S.C. § 1843(k); *see* also MARK SILBERGELD, CONSUMER FED'N OF AM., CFA HANDBOOK: FEDERAL AND STATE LEGAL PROTECTIONS OF CONSUMERS' FINANCIAL INFORMATION PRIVACY AND SECURITY 4–5 (2009).

[115] 15 U.S.C. §§ 6803, 6802(b) (2012). PayPal in fact adopts an opt-in policy respecting sales of personal information it collects to third parties. *Privacy Policy*, PAYPAL, https://cms.paypal.com/cgi-bin/marketingweb?cmd=_render-content&content_ID=ua/Privacy_full&locale.x=en_US (last visited Oct. 1, 2012).

[116] *Id.*

[117] *Id.*

[118] Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended in scattered sections of 18 U.S.C.).

[119] 18 U.S.C. § 2511.

[120] Stored Communications Act, 18 U.S.C. §§ 2701–12. This statute has assumed several names by different commentators. Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208, 1243 n.1 (2004). I've chosen the simplest.

[121] 18 U.S.C. § 2701.

[122] PAULA SELIS ET. AL., CONSUMER PRIVACY AND DATA PROTECTION: PROTECTING PERSONAL INFORMATION THROUGH COMMERCIAL BEST PRACTICES 2 (2002), *available at* http://www.atg.wa.gov/uploadedFiles/Home/Safeguarding_Consumers/Consumer_Issues_A-Z/Identity_Theft_(Privacy)/PrivacyPolicy.pdf ("In the United States there is no comprehensive privacy law that addresses the collection or use of personal information."). Although there are few laws on the books, the digital advertising industry has published self-regulation guidelines about online behavioral targeted advertising. AM. ASS'N OF ADVER. AGENCIES, ET AL., SELF-REGULATORY PRINCIPLES FOR ONLINE BEHAVIORAL ADVERTISING (2009), *available at* http://www.iab.net/media/file/ven-principles-07-01-09.pdf. Also, the Obama Administration, the FTC, and various members of Congress have proposed variations on a "Privacy Bill of Rights." THE WHITE HOUSE, CONSUMER DATA PRIVACY IN A NETWORKED WORLD: A FRAMEWORK FOR PROTECTING PRIVACY AND PROMOTING INNOVATION IN THE GLOBAL DIGITAL ECONOMY (2012); FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICY MAKERS (2012).

[123] Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003, 15 U.S.C. §§ 7701–13 (2012).

[124] *Id.* § 7704(a)(5).

vendor is required to obtain prior consent before it can send a marketing text to a mobile phone.[126]

On the English end, it is unlikely that the information about my web surfing or transaction was captured and maintained by British Telecom[127] or Google/U.K. longer than necessary to complete the transaction. That is because I did not opt-in to permit them to do so, and therefore, they likely could not establish a legitimate reason to retain the information under the data protection principles of Article 7 of the EU Directive.[128] In other words, the potentially valuable information about me and my transaction has, at least in principle, evaporated on the European side of the Atlantic before it can be used.[129] If the facts were reversed, so that I was placing an order from the U.S. to a vendor in England, the resulting rights would have been quite different. Without my express consent, the English vendor could not have retained records about my transaction longer than required to complete the transaction, could not have sold it to third parties, and could not have used it to make sales to me in the future.[130] Like the U.S. vendor, if the English vendor sent me commercial emails, it would be required to give me an opt-out right under the EU Directive on Privacy and Electronic Communication. ("E-Privacy Directive")[131] On the other hand, Google/U.S. could and undoubtedly would capture all the information about my Web surfing exercise, selling that information to its advertisers so that they can target ads to me the next time I log on to Google to do some fruit or Mother's Day shopping.[132] The value of this information in Google's hands—or Facebook's, or Amazon's—is directly measured by the lofty heights of their market capitalizations.[133] They are, in other words, profiting from my identity—who I am,

---

[125] 47 U.S.C. § 227.

[126] *Id.* § 227(b)(1)(A)(iii). Although not explicit in the statute, the FCC has clarified that § 227(b)(1)(A)(iii) includes text messages in addition to voice calls. *See* Rules and Regulations Implementing the Telephone Consumer Protection Act (TCPA) of 1991, 68 Fed. Reg. 44,144, 44,165 (July 25, 2003) (to be codified at 47 C.F.R. pts. 64 & 68). The CAN-SPAM Act also requires prior consent if the message uses an Internet address that includes an Internet domain name (usually the part of the address after the individual or electronic mailbox name and the "@" symbol). 15 U.S.C. § 7712.

[127] *See* Directive 2002/58, of the European Parliament and of the Council of 12 July 2002 on Privacy and Electronic Communications, 2002 O.J. (L 201) 37 (EC) [hereinafter E-Privacy Directive]. The E-Privacy Directive prohibits, among other things, traffic and location data about subscribers and users from being used for marketing or other purposes without the individual's consent. *Id.* arts. 6, 9.

[128] EU Directive, *supra* note 37, art. 7.

[129] *Id.*

[130] Data Protection Act, *supra* note 60, § 4, sch. 1.

[131] E-Privacy Directive, *supra* note 127, art. 13. Note that the English vendor could market to me via email only if it had obtained my email address via my prior transaction. Unlike the U.S. vendor. the English vendor could not have purchased my email address from someone else and then marketed to me without my consent. *See, e.g.*, Data Protection Act, *supra* note 60, § 17.

[132] JOHN F. TANNER & MARY ANNE RAYMOND, PRINCIPLES OF MARKETING ch. 3 (Flat World Knowledge ed., 2010), *available at* http://catalog.flatworldknowledge.com/bookhub/2030?e=fwk-133234-ch03#fwk-133234-ch03 (discussing consumer behavior and how they make buying decisions).

[133] *See, e.g.*, Erin Carlyle, *Larry Page's Fortune Up As Google Overtakes Microsoft in Market Cap*, FORBES (Oct. 1, 2012, 4:55 PM), http://www.forbes.com/sites/erincarlyle/2012/10/01/larry-pages-fortune-up-as-google-overtakes-microsoft-in-market-cap/.

what I'm interested in, what I buy—and I do not have any right to claim royalties on their profit.[134] In the U.S., this information about me is in some important sense theirs, not mine.[135] In England, it is a little less theirs, but hardly more mine.[136]

II. DIGITAL IDENTITY

One might think of a person's digital identity by analogy to a pointillist painting. Thousands upon thousands of tiny bits of digital information about an individual, including what we have called basic facts, sensitive facts, and transactional facts, can be assembled to form a picture of the individual: his likes, dislikes, predispositions, resources; and in fact, any facet of his personality that has had contact with the Internet.[137] The picture may vary, depending on the interest of the digital assembler of information and the access of that person to the individual's digital life,[138] but it will be a picture of identity nonetheless.

Who owns these pictures? We have already noted that the individual pieces of digital information are not owned, in any ordinary sense, by the individual generating them.[139] But what about the pictures as a whole? Who owns them? In some sense, the individual certainly created them, particularly as they relate to transactions effected on the Internet or information posted on the Internet. Does that mean that the individual owns them?[140]

Here we encounter something more closely akin to traditional notions of property rights, and the answer is a bit surprising. In Europe, the Database Directive,[141] adopted by the European Commission in 1996, requires member states

---

[134] *See* Bergelson, *supra* note 30, at 383.

[135] *See* sources cited *supra* note 109. The fact that a company holds the aggregated information about a customer compiled into a customer list as a trade secret indicates an ownership right in that information. *See* Hamilton-Ryker Grp., LLC v. Keymon, No. W2008-00936-COA-R3-CV, 2010 WL 323057, at *15–16 (Tenn. Ct. App. Jan. 28, 2010).

[136] *See* Kirsch, *supra* note 100, at 7–9. Not surprisingly, there are proposals to require consent before information about one's on-line behavior can be tracked for commercial purposes. *See id.* at 17–21.

[137] *See* Erica Newland, *Disappearing Phone Booths: Privacy in the Digital Age*, CENTER FOR DEMOCRACY AND TECH. (May 2012), https://www.cdt.org/files/pdfs/Privacy-In-Digital-Age.pdf (cataloguing various types of data capable of being tracked by third parties).

[138] *See* Mell, *supra* note 30, at 6.

[139] Bergelson, *supra* note 30, at 383; *see also* Laura A. Heymann, *The Law of Reputation and the Interest of the Audience*, 52 B.C. L. REV. 1341, 1342 (2011).

[140] I propose this question in part to test the theses that property rights either flow from the efforts of the individual, *see* JOHN LOCKE, TWO TREATISES OF GOVERNMENT 314 (Peter Laslett ed., Cambridge Univ. Press 1988) (1690), or manifest individuality and thus promote individual autonomy, *see* IMMANUEL KANT, THE METAPHYSICAL ELEMENTS OF JUSTICE 56 (John Ladd ed. & trans., Hackett Publ'g Co. 1999) (1797); MERGES, *supra* note 1, at 31–33, 68–77 (discussing the property concepts of John Locke and Immanuel Kant). What could be more personal, or more the product of my individual efforts, than my identity? Should it not, then, be my property?

[141] Directive 96/9 of the European Parliament and of the Council of 11 March 1996 on the Legal Protection of Databases, 1996 O.J. (L 77) 20 (EC) [hereinafter Database Directive].

to provide protection for databases.[142] U.K. regulations implementing the Database Directive expressly state that "[a] property right ('database right') subsists, in accordance with this Part, in a database if there has been a substantial investment in obtaining, verifying or presenting the contents of the database."[143] Similarly, the United States Copyright Act provides copyright protection for compilations so long as there is copyrightable authorship in their selection or arrangement.[144]

Therefore, the compilations of facts that comprise a person's digital identities are subject to ownership, but the owner is not the person; it is the compiler![145] Quite remarkably, the individuals who generate the information that comprises their digital identities do not own the databases, and therefore, in a very real sense, do not own their own identities.[146] Their identities, the images of which can vary from compiler to compiler, are owned by the companies who assemble the information into something useful and saleable.[147] The companies and enterprises that gather the information, package it, and make it available for exploitation and sale, often as an aggregation of individual compilations, own it and can profit from it.[148]

---

[142] *See id.* art 7. The European Commission published a report in 2005 questioning whether the Database Directive had been effective, but no further action has been taken to amend or improve it. *First Evaluation of Directive 96/9/EC on the Legal Protection of Databases* (Dec. 12, 2005), *available at* http://ec.europa.eu/internal_market/copyright/docs/databases/evaluation_report_en.pdf.

[143] The Copyright and Rights in Databases Regulations, 1997, S.I. 1997/3032, art. 13 (Eng.).

[144] 17 U.S.C. § 103 (2012).

[145] *Id.* To continue the analogy to Pointillism, Seurat surely owned copyright in his paintings, but not in the individual points of color of which they were composed. *See generally* Bergelson, *supra* note 30, at 404 (cataloguing court decisions acknowledging property rights of compilers of personal information). There is, of course, also the possibility that someone could be his own compiler, creating in effect a digital self-portrait. The personal pinboards created by users of www.Pinterest.com are an example. *See What is Pinterest?*, PINTEREST, http://pinterest.com/about/ (last visited Oct. 17, 2012). The individual Pinterest user creates his or her own profile of preferences by "pinning" images from other Pinterest pinboards or from other websites. *Id.*

[146] Dan Gillmor, *Google+ Forces Us to Question Who Owns Our Digital Identity,* THE GUARDIAN (July 13, 2011, 8:13 PM), http://www.guardian.co.uk/commentisfree/cifamerica/2011/jul/13/google-plus-online-identiy.

[147] SELIS ET. AL., *supra* note 122, at 9 ("A consumer's personal information has the potential of being bought and sold like any other valuable commodity.").

[148] *See* Tanzina Vega & Edward Wyatt, *U.S. Requests Tougher Rules on Data Sales*, N.Y. TIMES, Mar. 26, 2012, at A1. One can distinguish aggregations of facts about a single individual from aggregations of facts about multiple individuals, but the legal principles attaching to these aggregations are not different. *See* 17 U.S.C. § 103. People commonly focus on the second of these, and much of what is referred to as "Big Data" resides in such multiple-individual aggregations. *See supra* note 27. On the other hand, it is the aggregation of facts about particular persons that delivers real marketing value—who is this person? How old is she? How much money does she have? Where does she live? Where is she now? What does she typically like to buy? *See* Clair Cain Miller & Somini Sengupta, *In Mobile World, Tech Giants Scramble to Get Up to Speed*, N.Y. TIMES, Oct. 23, 2012, at A1 ("[M]obile provides huge opportunities for these businesses, industry analysts say.. That is largely because people reveal much more about themselves on phones than they do on computers, from where they go and when they sleep to whom they talk to and what they want to buy.").

The conclusion that one does not own one's own identity might seem jarring at first.[149] On further reflection, though, one realizes that the lack of ownership over one's digital identity is not very different from one's identity outside of the digital space.[150] Identity is an edifice built out of facts about one's self that are known to others—basic facts, sensitive facts, historical facts, genetic facts, relational facts, transactional facts. These facts can be influenced by the individual, but they are not owned by the individual, either individually or in the aggregate.[151]

Think of identity as reputation. Do I own my reputation? I have a reasonably broad opportunity to mold my reputation by word and deed, and I have legal redress if my reputation is unfairly tarnished,[152] but if I have committed a crime or a fraud, the people I deal with are entitled to know that and to protect themselves accordingly.[153] If on the other hand I have behaved in an exemplary fashion—paying my debts, respecting others, honoring contracts, avoiding litigation—others are entitled to know that as well. The individual might not want everyone to know the bad things, but the individual cannot in general prevent it. One's reputation is, to a large extent, the product of one's actions and initiative, but it is not, as a result, one's property.[154] It is, in a sense, community property.[155] The individual builds it, at

---

[149] *See* sources cited *supra* note 30. Indeed, this legal fact seems to have inspired legal scholars such as Mell and Bergelson to exert enormous efforts to propose legal property rights in PII or identity or both. *See id.*

[150] *See* Gill v. Hearst Publ'g Co., 253 P.2d 441, 444 (Cal. 1953) ("Consistent with their own voluntary assumption of this particular pose in a public place, plaintiffs' right to privacy as to this photographed incident ceased and it in effect became a part of the public domain . . . .").

[151] *See supra* note 82 and accompanying text.

[152] *See* Barrows v. Wareham Fire Dist., 82 Mass. App. Ct. 623, 627 (2012) ("[T]he gravamen of the tort of defamation does not lie in the nature or degree of the misconduct but in its outcome, i.e., the injury to the reputation of the plaintiff."). The remedy, of course, lies in the tort of defamation. RESTATEMENT (SECOND) OF TORTS § 558 (1977). There are well-known differences between the United States and the U.K. in the scope of this tort, driven largely by First Amendment considerations in the United States that do not apply in the U.K. *See* Doug Rendleman, *Collecting a Libel Tourist's Defamation Judgment?*, 67 WASH. & LEE L. REV. 467, 478–80 (comparing U.S. and U.K. defamation laws); *compare* N.Y. Times Co. v. Sullivan, 376 U.S. 254, 269–71 (1964) (discussing that there must be a freedom to speak openly, especially in debates and criticism, even when that speech may not have been proven to be true), *with* Defamation Act, 1996, c. 31 (Eng.) (discussing the law of defamatory statements without making reference to any right or freedom to speak openly regardless of the context in which the defamatory statements were made).

[153] *See* Sandra D. Scott, *What is a Police "Investigative Report"?*, 51 J. MO. B. 83, 84 (1995) (discussing one State's policy of informing the public about crimes in the community). In the U.K., evidence about criminal prosecutions is considered sensitive personal information and is therefore subject to special protections. Data Protection Act, *supra* note 60, § 2. With the exception of juvenile crimes, there is no comparable principle in the U.S. *See, e.g.*, Hodge v. Jones, 31 F.3d 157, 166 (4th Cir. 1994) ("[C]riminal records are matters of public record, easily obtained upon request, and . . . there is no automatic right to expunction thereof . . . ."); Joanna S. Markman, *In Re Gault: A Retrospective in 2007: Is It Working? Can It Work?*, 9 BARRY L. REV. 123, 127 & 141 n.29 (2007) (discussing the confidentiality of juvenile records).

[154] Heymann, *supra* note 139, at 1342. This conception diverges sharply from John Locke's view that the admixture of personal effort with raw material justifies property rights, or even Immanuel Kant's conception of property as the manifestation of individual liberty. *See* MERGES, *supra* note 1, at 31–33, 68–77.

[155] Heymann, *supra* note 139, at 1342 ("[R]eputation is a social creation dependent on intergroup communication."). Note in this connection that one's identity can be ascertained and

least in part, but the community members can then use it—or decide that it would be unfair or unjust to use it—whether the individual wants them to or not.[156]

We can also return here to the analogy to trademark law. Trademark rights attach to the "good will" associated with a vendor and its products.[157] The good will of a business is listed as one of its assets;[158] indeed, it may be the business's largest asset, but it is utterly reliant on the public's perception of the business.[159] By change of heart, or even by generic use, the public at large can destroy this "asset," and the business has no legal recourse whatsoever.[160]

We might also return to our watershed analogy. No one owns the raindrops falling on the watershed, but when value is created by damming streams of information, that value can be owned and exploited by the persons building and running the dams. Eventually, of course, the information returns to the oceanic public domain.

A. The Exploitation of Identity

If it is jarring to consider that one's digital identity is owned by others, not by one's self, it is still more disturbing to consider what the owners might do with their information. It is one thing for Amazon to keep track of the books you bought and to use that information to identify other books you might like to buy. This is not too different from the proprietor of a local bookstore (if there remains one that has not yet been put out of business by Amazon) telling you that he just got in a book by an author he knows you will like. This is good customer service, as long as it is not too insistent. It would be quite another thing for the local bookseller to ring up his friend, the kitchenware merchant across the street, and tell him you just bought a cookbook that requires a particular utensil that the merchant might want to sell to him. The latter has the feel of an invasion of privacy.[161] This is of course exactly

---

owned by anyone who has the ability and takes the trouble to assemble the relevant facts. *See* 17 U.S.C. § 103. Like any other compilation of data, another person can access the same or similar data and assemble its own compilation, without infringing the property rights of the first compiler. *Id.* An image of one's identity can be owned by anybody taking the trouble to compile it. *Id.*

[156] *See* Heymann, *supra* note 139, at 1342. Merges struggles a bit to bring intellectual property within John Rawls' framework for a just society. MERGES, *supra* note 1, at 102–05 (discussing JOHN RAWLS, A THEORY OF JUSTICE (Harv. Univ. Press rev. ed. 1999)). It is far easier to bring the non-property concept of identity/reputation proposed in the text within the framework of what persons in the "original position" would agree upon. They could well agree, for example, that the community ought to have ready access to most reputational facts, but that it would be unwise to permit the free exchange of sensitive personal information that is subject to misuse, or that could easily be used to the disadvantage of the least fortunate in society (Rawls' Second Principle). *Id.* at 104.

[157] Heymann, *supra* note 139, at 1343.

[158] *See* 1 MCCARTHY, *supra* note 16, § 2.19.

[159] *See id.*

[160] *See* 15 U.S.C. § 1064 (2012) (allowing a petition to be filed for the cancellation of a registered trademark if it becomes the generic name the public uses for a good or service).

[161] The Fair and Accurate Credit Transactions Act of 2003 ("FACTA"), an amendment to the Fair Credit Reporting Act, prohibits companies from using certain credit information received from an affiliate to market goods or services to a consumer, unless the consumer is given notice, a

what Amazon is doing all the time,[162] and in important part, what legislatures and regulators react to with the plethora of privacy laws we have today.[163] The problem is not that the bookseller or Amazon have and own information about your purchase. The problem is what they do with it.[164]

One sees a somewhat different issue in Facebook's "Sponsored Stories" service. In this service, Facebook features in advertisements the name and picture of Facebook friends who click a button to show they "like" something, charging a fee to the provider of the thing that was "liked."[165] Facebook does not share its revenue with the person doing the "liking."[166] This prompted a class action lawsuit, which Facebook settled by agreeing to give notice to its users that their preferences would be exploited in this way, coupled with an opt-out right.[167] The problem here cannot be considered an invasion of privacy. Surely the people who tap "like" intend for their positive response to be known at least by their "friends," even if they have not read the fine print of Facebook's terms of use. The problem is more directly related to the exploitation of a person's identity for profit, which squarely implicates state right of publicity laws that generally require consent before a person's name or image can be used for commercial purposes.[168] It is worth noting that Facebook did not agree to discontinue the Sponsored Sites service.[169] Its settlement simply made it clearer to Facebook users that one of the quid pro quos for their free Facebook service was, in effect, a license to use their names and likenesses for commercial purposes.[170]

If a person pays with anything other than cash, there is also the question whether the vendor has safeguarded the credit card or bank information. Security

---

reasonable opportunity to opt-out, and a simple and reasonable method for opting-out (the FTC Affiliate Sharing Rule). Fair and Accurate Credit Transactions Act of 2003, Pub. L. No. 108-159, sec. 214, § 624, 117 Stat. 1952, 1980–82 (codified as amended at 15 U.S.C. § 1681s-3); *see also FTC Approves Affiliate Marketing Rule Regarding Use of Consumer Information*, FED. TRADE COMMISSION (Oct. 23, 2007), http://www.ftc.gov/opa/2007/10/affiliate.shtm.

[162] Nick Eaton, *Suit: Amazon Fraudulently Collects, Shares Users' Personal Info*, SEATTLEPI.COM, http://www.seattlepi.com/business/article/Suit-Amazon-fraudulently-collects-shares-users-1040886.php (last updated Mar. 2, 2011).

[163] *See, e.g.*, Do Not Track Me Online Act of 2011, H.R. 654, 112th Cong. (2011); Commercial Privacy Bill of Rights Act of 2011, S. 799, 112th Cong. (2011); BEST PRACTICES Act, H.R. 611, 112th Cong. (2011); Consumer Privacy Protection Act of 2011, H.R. 1528, 112th Cong. (2011); Do-Not-Track Online Act of 2011, S. 913, 112th Cong. (2011); Do-Not-Track-Kids Act, H.R. 1895, 112th Cong. (2011).

[164] Hardly a day goes by without a new revelation about the use of personal information or the unauthorized disclosure of sensitive personal information. *See, e.g.*, Natasha Singer, *You For Sale*, N.Y. TIMES, June 17, 2012, at BU1 (raising concerns about Acxiom gathering personal information from customers and selling it to marketers for targeted advertising when there have been multiple security breaches).

[165] *Daily Report: What's Behind Facebook's Sponsored Stories*, N.Y. TIMES BITS (June 1, 2012, 6:44 AM), http://bits.blogs.nytimes.com/2012/06/01/daily-report-whats-behind-facebooks-sponsored-stories/.

[166] *See id*. The quid pro quo is the free service provided by Facebook to its users.

[167] Somini Segupta, *To Settle Lawsuit, Facebook Alters Policy for Its Like Button*, N.Y. TIMES, June 22, 2012, at B2.

[168] 4 LOUIS ALTMAN & MALLA POLLACK, CALLMANN ON UNFAIR COMPETITION, TRADEMARKS & MONOPOLIES § 22:32 (4th ed. 1981).

[169] *See* Segupta, *supra* note 167.

[170] *Id*.

breaches are distressingly common. In June of 2012, the FTC filed a complaint against Wyndham Hotels for security lapses that allowed hackers to access sensitive financial information of more than 600,000 individuals over a three-year period.[171] In the same month, LinkedIn, eHarmony, and Last.fm were all hacked, resulting in the release of millions of users' passwords,[172] and just three months before, the credit card processor Global Payments reported that some 1.5 million Visa and MasterCard account numbers had been stolen by hackers.[173] Even breaches of less sensitive information, such as that of Epsilon in which the email addresses of millions of individuals were inadvertently disclosed, are disturbing and potentially harmful to individuals.[174]

Many of the laws respecting PII can thus be understood as limitations on the ownership rights of, and the creation of liability for, the persons, or rather businesses, that assemble and own collections of PII. One might analogize the collections of PII that comprise one's digital identities to dangerous instrumentalities.[175] It is okay to build and own them; indeed, their creation represents the generation of an important new form of wealth in the Internet Age, but the use of such information must be regulated to avoid harm or unlawful exploitation. The www.pleaserobme.com episode is an example. The pleaserobme.com website scraped Twitter messages that had been pushed through the FourSquare social media site to provide a real-time list of people who were not at home.[176] The site apparently intended to raise awareness of the vulnerabilities created by location information, but its potential for abuse is obvious.[177] Facebook offered, for one day, a service called "Find Friends Nearby" that allowed Facebook

---

[171] Complaint for Injunctive and Other Equitable Relief, Fed. Trade Comm'n v. Wyndham Worldwide Corp., No. 12-cv-01365 (D. Ariz. June 26, 2012), *available at* http://www.ftc.gov/os/caselist/1023142/120626wyndamhotelscmpt.pdf. The gravamen of the complaint, which alleged losses to customers exceeding $10 million, *id.* ¶ 2, was that Wyndham's privacy policy misrepresented its data security precautions, which, it turned out, had essentially nil with personally identifiable financial information stored in plain text. *Id.* ¶¶ 24, 40.

[172] Sara Yin, *Last.FM Joins eHarmony, LinkedIn to Celebrate Breach Week*, SECURITYWATCH (June 7, 2012, 6:36 PM), http://securitywatch.pcmag.com/none/298865-last-fm-joins-eharmony-linkedin-to-celebrate-breach-week.

[173] Brian Krebs, *MasterCard, VISA Warn of Processor Breach*, KREBS ON SECURITY (March 30, 2012, 1:23 AM), http://www.krebsonsecurity.com/2012/03/mastercard-visa-warn-of-processor-breach/.

[174] *See, e.g.*, Singer, *supra* note 164.

[175] *See* Stecyk v. Bell Helicopter Textron, No. 94-CV-1818, 1998 U.S. Dist. LEXIS 609, at *15 n.4 (E.D. Pa. Jan. 26, 1998) (defining a dangerous instrumentality as "anything which has the inherent capacity to place people in peril, either in itself (e.g. dynamite), or by a careless use of it (e.g. boat)").

[176] *See* Caroline McCarthy, *The Dark Side of Geo: PleaseRobMe.com*, CNET NEWS (Feb. 17, 2012, 9:55 AM), http://news.cnet.com/8301-13577_3-10454981-36.html.

[177] *Id.*

users to see which friends were nearby.[178] It took the service down because of very real concerns over stalking.[179]

That this is the case is manifest in the basic principles of privacy legislation as diverse as the EU Directive, the Fair Credit Reporting Act, HIPAA, Gramm-Leach-Bliley, and the Massachusetts Data Security Regulations. In each case, the assembly of personal information about individuals is not prohibited.[180] Quite to the contrary, such assemblies are affirmatively encouraged, particularly in the areas of financial services and health care, because the information can greatly improve the efficient and effective provision of financial and health services.[181] The use of the information, however, is regulated and controlled once assembled.[182]

The regulations and controls fall into two broad classes: (1) requirements for the security of such information, particularly when it falls into the "sensitive" categories mentioned above, and (2) regulation over the dissemination of such information to third parties. In the first of these categories one finds the example of the Massachusetts Data Security Regulations, which directly specify minimum security standards to preclude the unauthorized disclosure of PII,[183] HIPAA, which mandates a variety of security standards for health information,[184] and the payment card data security standard ("PCI DSS"), which is enforced through contracts among payment card companies, banks, and merchants.[185] Laws that require prompt notice of the unlawful disclosure of personal information fall into the same category.[186]

The second class of control over the use of PII held by third parties inheres in the variety of conditions that we have already seen on the use and distribution of PII. These include the almost universal requirement that individuals be provided with

---

[178] *See* John D. Sutter, *Facebook Quietly Unveils "Stalking App,"* CNN TECH (June 29, 2012), http://www.cnn.com/2012/06/25/tech/social-media/facebook-find-friends-nearby/index.html?hpt=hp_bn5. The service was aptly dubbed "the stalking app" by the blog ReadWriteWeb. *Id.*

[179] *Id.*

[180] EU Directive, *supra* note 37, art. 6 (stating that personal data "must be . . . collected for specified, explicit, and legitimate purposes"); 15 U.S.C. § 1681(b) (2012) (stating the Congressional purpose of the FCRA is to require consumer reporting agencies to collect information "in a manner which is fair and equitable to the consumer"); 45 C.F.R. § 164.502 (2012) (setting forth permissible uses of medical information, under the assumption that such information should be collected); 15 U.S.C. § 6802 (setting forth obligations of financial institutions in handling consumer information, under the assumption that such information should be collected); 201 MASS. CODE REGS. 17.01–.05 (2012) (providing conditions for ownership of non-public information).

[181] *See* 45 C.F.R. § 164.502; 15 U.S.C. § 6802.

[182] *See, e.g.*, 42 U.S.C. § 1320c-9 (regulating disclosure of personal information possessed for medical purposes).

[183] 201 MASS. CODE REGS. 17.03–.04.

[184] 45 C.F.R. § 164.306.

[185] *See PCI SSC Security Standards Overview*, PCI SECURITY STANDARDS COUNCIL, https://www.pcisecuritystandards.org/security_standards/ (last visited Oct. 18, 2012).

[186] *See, e.g.*, CAL. CIV. CODE §§ 1798.80–.84 (West 2012) (explaining the California breach notification law); N.Y. GEN. BUS. LAW §§ 899-aa(3)–(4) (McKinney 2012) (explaining the New York data breach notification law); TEX. BUS. & COM. CODE § 521.053 (West 2012) (explaining the Texas data breach notification law); 815 ILL. COMP. STAT. 530/5 (2012) (explaining the Illinois data breach notification law). Breach notification is also required by HIPAA and its implementing regulations. *See* 45 C.F.R. §§ 164.404–.405 (2012).

notice of the uses to which their PII will be put and the requirement that there be a division between opt-in and opt-out requirements for the use or disclosure of that information.[187] One might consider these requirements as something falling at least partly into the realm of consumer education for the digital age. It is not so much that the collection and exploitation of consumer information is an inherently obnoxious activity—we consider it good service to know one's customers and to endeavor to respond to them personally—but that the facility with which such information can be collected and disseminated for profit comes as a great and sometimes unpleasant surprise.[188] Notice at least diminishes the surprise. It also provides a basis for consent where laws, such as the right of publicity, require it.[189]

All of these restrictions can be understood as limitations on the uses to which the owner of the collections of PII that we are referring to as "digital identity" can put that information. This is analogous to the limitations that are imposed on the owners of a wide variety of other types of property, particularly when the property is capable of causing harm.[190] If, for example, you own a car, you must register it to drive on the public roads, drive on the proper side of the road, use your turn signals before you turn, and not exceed the speed limit.[191]

B. Countervailing Considerations

Let us take stock in where our reasoning has brought us. Digital identity comprises a collection of thousands of facts about a person, and that person does not own those facts.[192] The facts can be assembled in many ways, each giving a somewhat different picture of the person—an image, as it were, in a different light or from a different direction. The law gives the assemblers of those facts, not the individual, ownership of those digital images.[193] There is a somewhat uncertain right to complain about it if some of the facts comprising the image are untrue[194] or if their

---

[187] *See, e.g.*, 15 U.S.C. § 6802(a)–(b) (2012).

[188] *See, e.g.*, Miguel Helft, *Critics Say Google Invades Privacy with New Service*, N.Y. TIMES, Feb. 13, 2010, at B1 (describing public backlash after release of "Google Buzz," a service that used e-mail and chat data to automatically publish users' contacts without notice or consent).

[189] *See* Jones v. Corbis Corp., 815 F. Supp. 2d 1108, 1111 (C.D. Cal. 2011) *aff'd*, No. 11-56082, 2012 WL 2884790 (9th Cir. July 16, 2012) ("Notices are sometimes posted at these events stating that celebrities entering the red carpet consent to being photographed and recorded, and also to having their name or likeness used in connection with the event."); CAL. CIV. CODE § 3344 (prohibiting the use of a person's identity without that person's prior consent, and not requiring the consent to be in writing).

[190] *See, e.g.*, 18 U.S.C. § 923 (imposing a federal licensing requirement on gun ownership and limiting the use of guns even after they are licensed).

[191] *See, e.g.*, 625 ILL. COMP. STAT. 5/11-100 to 1516.

[192] *See* Bergelson, *supra* note 30, at 403 ("Currently, neither property nor torts theory recognizes individuals' rights in their information.").

[193] *See supra* notes 180–182 and accompanying text.

[194] *See, e.g.*, 5 U.S.C. § 552a(d) (2012); 15 U.S.C. §§ 1681g, 1681i.

use offends policy,[195] but one cannot, in general, complain about the assembly of the images as a whole. At the same time, the law imposes some rather strict limits on what the assembler can do with these images.[196] One might say that these assemblies of facts are dangerous instrumentalities, and the misuse of them can give rise to both strict liability and liability for negligence if they are not used carefully.

Is this a reasonable outcome? Many scholars argue that there should be property rights in identity.[197] Robert Merges, for example, cites the development of a right of publicity as an example of the creation of a property rights.[198] In its original form, the right of publicity attaches to what one might call a persona: an artifice built around a person as a result of fame, notoriety, and in many cases the efforts of teams of publicists.[199] Fair enough. If a public persona is as much the creation of a work as is a character in a novel, why should the persona not have the same level of protection, more like a copyrighted work, and less like a trademark? This point can be taken, but at the same time, it does not equate to saying that facts about the person behind the persona also belong to him or her, nor that a construct built of those facts should belong to him or her. And, in fact, persons who have property-like rights in their public personas have virtually no ability to exclude third parties from facts about their real selves.[200]

State laws protecting the "right of publicity" present a higher obstacle to this response because they are not typically limited to famous people; instead, they typically attach to the use of *any* person's name or likeness for commercial

---

[195] See, for example, Biddle v. Warren Gen. Hosp., 715 N.E.2d 518, 523 (Ohio 1999), for a discussion of numerous jurisdictions that have recognized a common law tort for the unauthorized disclosure of confidential medical information.

[196] *See, e.g.*, 201 MASS. CODE REGS. 17.03–.04 (2012) (requiring any entity that deals in personal information to implement robust, multi-faceted security measures to protect that information).

[197] *See* Sarah Ludington, *Reining in the Data Traders: A Tort for the Misuse of Personal Information*, 66 MD. L. REV. 140, 143–46 (2006) (discussing data trading and the debate among academics about protecting personal information through property rights).

[198] Merges, *supra* note 1, at 96–101.

[199] 1 MELVILLE B. NIMMER & DAVID NIMMER, NIMMER ON COPYRIGHT § 1.01[B][1][c] ("The 'work' that is the subject of the right of publicity is the *persona*, *i.e.*, the name and likeness of a celebrity or other individual.") (emphasis in original). The right of publicity is currently a state law-based right. Nineteen states recognize the right by statute: California, Florida, Illinois, Indiana, Massachusetts, Kentucky, Nebraska, Nevada, New York, Ohio, Oklahoma, Pennsylvania, Rhode Island, Tennessee, Texas, Utah, Virginia, Washington, and Wisconsin. *Statutes*, RIGHT OF PUBLICITY, http://www.rightofpublicity.com/statutes (last visited Oct. 1, 2012). Twenty-one states have recognized the right by common law (though it has been replaced by statute in some states): Alabama, Arizona, California, Connecticut, Florida, Georgia, Hawaii, Illinois, Kentucky, Michigan, Minnesota, Missouri, New Hampshire, New Jersey, Ohio, Pennsylvania, South Carolina, Texas, Utah, West Virginia, Wisconsin. 1 J. THOMAS MCCARTHY, RIGHTS OF PUBLICITY AND PRIVACY § 6.3 (2d ed. 2012); *see also* RESTATEMENT (THIRD) OF UNFAIR COMPETITION §§ 46–49 (1995) (discussing the right of publicity and its protection through statutory and common law and mentioning several states that use the common law right of publicity protection).

[200] *See* Midler v. Ford Motor Co., 849 F.2d 460, 462 (9th Cir. 1988) ("The purpose of the media's use of a person's identity is central. If the purpose is 'informative or cultural' the use is immune; 'if it . . . merely exploits the individual [it is not].'" (quoting Peter L. Felcher & Edward L. Rubin, *Privacy, Publicity, and the Portrayal of Real People by the Media*, 88 YALE L.J. 1577, 1596 (1979))).

purposes.[201] This does not, however, establish that individuals own their digital identities. In the first place, publicity laws are almost always applied to the use of persons' names and likenesses as endorsements in advertisements;[202] they are not applied or understood to apply to the more indirect use of information about a person for other commercial purposes. Furthermore, their reach is limited to names and likenesses, and does not extend to transactional information about individuals.[203]

In recognition of the limitations of privacy and publicity law, two scholars—Vera Bergelson and Patricia Mell—argue at great length, and with impressive thoroughness, that a property right should attach to personal information, in the Bergelson's case,[204] or to "electronic persona" in the Mell's case.[205] At the risk of injustice by brevity to Bergelson's extended analysis, one might summarize that she believes that a tort remedy for invasion of privacy is inadequate and that the transaction costs of requiring data compilers to obtain the permission of their data subjects are not worse than the transaction costs of the subjects trying to prevent the compilations. She believes that, at bottom, it is unjust for third parties to profit from the individuality of the persons whose personal information resides in the third parties' databases:

> In a nutshell, the suggested legal regime would give individuals property rights in their personal information. They would own this information during their lifetime, subject to a (i) non-exclusive automatic inalienable license to the original collector and (ii) limited non-exclusive automatic license to the general public. This way, friends of, say, Robert Bork would be free to talk, and newspapers free to write, about movies he watches or books he reads, but a video- or bookstore would not be free to reveal his customer record even in the heat of his nomination campaign.[206]

---

[201] *See* N.Y. CIV. RIGHTS LAW § 51 (McKinney 2012) (regulating use of "any person['s]" identifying features); CAL. CIV. CODE § 3344 (West 2012) (proscribing use of "another's" identifying features); Doe v. TCI Cablevision, 110 S.W.3d 363, 369 (Mo. 2003) (stating the elements of a common law cause of action for violation of the right of publicity as follows: "(1) [t]hat defendant used plaintiff's name as a symbol of his identity (2) without consent (3) and with the intent to obtain a commercial advantage"). *But see* IND. CODE § 32-36-1-6 (2012) (limiting regulation to people whose identifying features have "commercial value").

[202] *See* I. J. Schiffres, Annotation, *Invasion of Privacy by Use of Plaintiff's Name or Likeness in Advertising*, 23 A.L.R.3d 865 § 2[a] (1969). This is what got Facebook into trouble with its Sponsored Stories service. *See supra* notes 165–170.

[203] *See* N.Y. CIV. RIGHTS LAW § 51 (providing relief for the use of a person's "name, portrait, picture, or voice" without consent); CAL. CIV. CODE § 3344 (holding a person liable for damages for the unauthorized use of another's "name, voice, signature, photograph, or likeness"); IND. CODE § 32-36-1-6 (defining "personality" to mean a "person whose name, voice, signature, photograph, image, likeness, distinctive appearance, gestures, or mannerisms has commercial value" (numbering omitted)).

[204] *See generally Bergelson, supra* note 30 (arguing that individuals should have property rights in their personal information). Bergelson lists works that have focused on the social utility of granting individuals property rights in personal information. *Id.* at 383 n. 16. She also discusses defining rights to personal information based on torts or property. *Id.* at 414–19.

[205] Mell, *supra* note 30, at 68–70.

[206] Bergelson, *supra* note 30, at 442.

Bergelson's qualifications (i) and (ii) on the individual's "property" interest in her personal information are so broad as to make one wonder whether it is a property interest at all.[207] If Robert Bork's friends and newspapers can trade in the same information that is in the possession of the bookstore, can it reasonably be said that the information belongs to him? Bergelson may be unhappy about the bookstore's disclosure of information about Bork's purchases and may want to create a remedy for it, but if the information were really his, it should not matter who had misappropriated it—the friend, bookstore or newspaper.

Bergelson's analysis also conflates the assembly of information that constitutes one's digital identity with the bits of information that go into that assembly. She dislikes the fact that persons putting together the assembly can profit from it, whereas the individuals cannot.[208] In effect, she reasons that if there is a property interest in the collection of data, then there ought to be a property interest in the individual bits of data it comprises.[209] But this may prove too much. Copyrights are granted in collections of facts, none of which individually are subject to ownership, whether via copyright or otherwise.[210]

Mell's position is bolder. While Bergelson acknowledges the right of the "first collector" to information about an individual, Mell wants even the first collector to be required to obtain the individual's consent to collect the information:

> The persona should be viewed as property, the ultimate "ownership" or "fee simple" of which resides in the individual. The rights of any other entity (i.e., any group, class, association or government) that might obtain, access, make use of or disclose the persona would be subordinate to those of the individual. As with other forms of property, the individual's right to restrict the use of his persona by others would vary depending upon the reason for the use.[211]

Fortunately, her definition of "persona" is limited to "a personal information file electronically stored, which, by virtue of at least one 'identifier,' relates the personal information to a specific person."[212] Were it not for this, she would have created a property interest in others' memories and diaries. She was also writing before the advent of iPads, iPhones, Droids, the Cloud, and the myriad other new electronic devices by which memories and images are stored these days.[213] Putting these

---

[207] Bergelson distinguishes her property interest from the "fee simple" proposed by Patricia Mell. *Id.* at 438; Mell, *supra* note 30, at 76.

[208] Bergelson, *supra* note 30, at 383 ("[O]n the one hand, [individuals] are powerless to prevent [their information's] unauthorized dissemination, and on the other, they are excluded from its profitable commercial exchange.").

[209] *Id.* at 419 (quoting Alice Haemmerli, *Whose Who? The Case for a Kantian Right of Publicity*, 49 DUKE L.J. 383, 418 (1999)).

[210] Feist Publ'ns, Inc. v. Rural Tel. Serv. Co., 499 U.S. 340, 344–45 (1991).

[211] Mell, *supra* note 30, at 76.

[212] *Id.* at 4.

[213] *See, e.g.*, Michael Chertoff, *Cloud Computing and the Looming Global Privacy Battle*, WASH. POST OPINIONS (Feb. 9, 2012), http://www.washingtonpost.com/opinions/cloud-computing-sets-stage-

anachronistic considerations aside, her conception, like Bergelson's, upends the basic principle that people who collect facts own their collections, whether the facts are human, botanical, zoological, commercial, or of any other nature.[214] The nasty fact is that other people can learn things about us, and we cannot easily make them forget or keep quiet about what they learn. The best we can do is to try to restrain abuses that are not justified by legitimate interests.

One must also return to the distinctions between the rights of privacy and publicity, on the one hand, and a property right in personal identity on the other. There is no question that the rights associated with PII are almost universally identified with a right of privacy—the right not to have unconsented intrusions into or publications of one's personal affairs.[215] In cases such as Facebook's Sponsored Stories service, they are also associated with the right of publicity—the right not to have one's name or likeness used in advertisements without consent.[216] As discussed above, the history of the development of the law of privacy and publicity, as manifest in the current regulation of PII, has not required the creation of an individual's property right, either in PII or in assemblies of PII comprising his digital identity.[217]

It is well known that the concept of a right of privacy, now manifest in all of the laws surveyed in this paper, was first elaborated by Louis Brandeis and Samuel Warren in their celebrated law review article, *The Right to Privacy*.[218] In their article, Brandeis and Warren considered and then rejected whether the right to privacy is a species of property:

> These considerations lead to the conclusion that the protection afforded to thoughts, sentiments, and emotions, expressed through the medium of writing or of the arts, so far as it consists in preventing publication, is merely an instance of the enforcement of the more general right of the individual to be let alone. It is like the right not be assaulted or beaten, the right not to be imprisoned, the right not to be maliciously prosecuted, the right not to be defamed. In each of these rights, as indeed in all other rights recognized by the law, there inheres the quality of being owned or possessed —and (as that is the distinguishing attribute of property) there may be some propriety in speaking of those rights as property. But, obviously, they bear little resemblance to what is ordinarily comprehended under that term. The principle which protects personal writings and all other personal

---

for-a-global-privacy-battle/2012/02/06/gIQAhV2V2Q_story.html (describing the impact of cloud computing on the issue of digital privacy).

[214] *Feist*, 499 U.S. at 345.

[215] *See* RESTATEMENT (SECOND) TORTS § 652A (1977). William L. Prosser identifies four species of privacy claims, which eventually found their way into the Restatement: false light, intrusion upon seclusion, public disclosure of embarrassing facts, and the appropriation of a name or likeness. WILLIAM L. PROSSER ET AL., PROSSER AND KEETON ON TORTS 851–68 (5th ed. 1984).

[216] *See* Fraley v. Facebook, Inc., 803 F. Supp. 2d 785, 806 (N.D. Cal. 2011).

[217] *See* Mell, *supra* note 30, at 8.

[218] Warren & Brandeis, *supra* note 82. The authors were motivated to propound their privacy thesis by "recent inventions and business methods" that "call attention to the next step that must be taken for the protection of the person." *Id*. at 195. They were concerned about photography and unscrupulous newspapers. *Id*. Imagine their shock if confronted with the Internet!

> productions, not against theft and physical appropriation, but against publication in any form, is in reality not the principle of private property, but that of an inviolate personality.[219]

It is worth noting that, in 1890, Brandeis and Warren were not even comfortable with the notion that copyright is a species of property.[220] They were, of course, writing at a time when the only protection for unpublished works was the common law right of first publication,[221] and it is easy to understand how they perceived a parallel between that right—really, a right to prevent disclosure—and a right of privacy. Statutory copyright has, since then, subsumed the common law right within the larger rubric of copyright ownership,[222] which, as we have seen, arguably has more of the characteristics of property ownership.[223] One might imagine that 120 years from now the privacy rights associated with some of the personal information that comprises one's digital identity will have grown into something closer to a property right in one's identity, and there are certainly forces pushing in that direction, but it has not happened yet.

One might also consider whether the emergence of "identity theft" laws[224] disproves this thesis.[225] If something is capable of being stolen, and if one can remedy the theft, does this not imply that it was owned in the first place?[226] The answer is likely no, and the proof is in the more ancient laws against fraud.[227] Fraudsters have been around for a very long time, and have run out of town on rails when they are uncovered.[228] Persons who steal identity in the electronic age have democratized fraud, and have brought the harm to bear more directly on the persons whose identities have been misappropriated, but the crime is essentially the same.

---

[219] *Id.* at 205.

[220] *Id.* at 200–04.

[221] *See* Caliga v. Inter Ocean Newspaper Co., 215 U.S. 182, 188 (1909) ("At common-law, the exclusive right to copy existed in the author until he permitted a general publication. Thus, when a book was published in print, the owner's common-law right was lost. At common-law an author had a property in his manuscript . . . .").

[222] *See* 17 U.S.C. § 106 (2012).

[223] *See* 17 U.S.C. § 201.

[224] *See, e.g.*, 18 U.S.C. § 1028.

[225] *See generally* Jennifer Lynch, *Identity Theft in Cyberspace: Crime Control Methods and Their Effectiveness in Combating Phishing Attacks*, 20 BERKELEY TECH. L.J. 259, 259–60 (2005) (explaining that phishing e-mails ask the recipient to verify personal information on a fake website, acting as the real business with the real account, in order to "steal her identity," suggesting that the identity was owned in the first place).

[226] Bergelson, *supra* note 30, at 404. Bergelson acknowledges that despite the name "identity theft," what the laws "really aim at is future crime (e.g., theft, fraud) the commission of which is facilitated by identity theft." *Id.* She points out that as long as there is no "intent to commit [a] future crime, an unlawful use or transfer of identifying information does not constitute a theft of identity," which suggests that the identity of a person is not truly owned. *Id.*

[227] *See, e.g.*, Commonwealth v. Boynton, 2 Mass. (1 Tyng) 77, 79 (1806) (finding defendant liable for common law fraud for counterfeiting the signatures of a bank president and cashier). Naturally, this is long before any identity theft laws were in place, yet pretending to be someone, albeit through signature, was still unlawful. *Id.*

[228] *See* MARK TWAIN, HUCKLEBERRY FINN, ch. 17 (The Duke and the Dauphin).

And, in effect, it proves my point: You cannot make yourself into somebody that you are not, and you cannot prevent people from knowing who you are.

III. SOME MODEST PROPOSALS

The collection and exploitation of PII continues to attract intense legislative and regulatory attention. The Appendix to this article catalogues bills pending in the U.S. Congress alone as of November 2012. Many dozens of bills are pending in state legislatures across the country, and the Information Commissioners of Europe proliferate their own interpretations, and re-interpretations, of the European Directives and implementing legislation.[229]

Recent initiatives of the Federal Trade Commission ("FTC") and the White House bear special mention. The White House published a White Paper in February of 2012, proposing a Consumer Privacy Bill of Rights, enforceable industry codes of conduct, effective enforcement by the FTC, and global harmonization of privacy laws.[230] In March of 2012, the FTC published its Report entitled "Protecting Consumer Privacy in an Era of Rapid Change."[231] The Report proposed a "Privacy Framework" comprising three elements: "Privacy by Design," "Simplified Choice," and "Greater Transparency."[232] For the most part, the FTC's framework was consistent with the White House's "Bill of Rights." Both call for greater individual control, transparency, simplified choice, improved security, and a reasonable connection between the information collected and the context in which it is collected.[233] The FTC also recommends enactment of "Do not Track" legislation that would provide consumers a means of preventing behavioral tracking.[234]

If one were to risk an overgeneralization, the FTC and White House proposals are, in comparison with their European counterparts, more concerned with education of consumers as to how their information is collected and used and less with limits over the actual collection and use of the information. This is, of course, consistent with the more *laissez faire* attitude that the United States takes to commerce in general.[235] It also, though, reflects the underlying reality that the collection and exploitation of personal data in the United States ran well ahead of the public's understanding of it,[236] whereas in Europe the EU Directive both educated the public

---

[229] To catalogue all the pending legislation, regulations and initiatives would convert this essay into a compendium.

[230] THE WHITE HOUSE, CONSUMER DATA PRIVACY IN A NETWORKED WORLD: A FRAMEWORK FOR PROTECTING PRIVACY AND PROMOTING INNOVATION IN THE GLOBAL DIGITAL ECONOMY 1–3 (2012) [hereinafter WHITE HOUSE WHITE PAPER].

[231] FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS (2012) [hereinafter FTC REPORT].

[232] *Id.* at vii–ix.

[233] *See* FTC REPORT, *supra* note 231, at vii–ix; WHITE HOUSE WHITE PAPER, *supra* note 230, at 1–2.

[234] *See* FTC REPORT, *supra* note 231, at 4. Do-not-track bills were filed in both the House and Senate in 2011. *See* Appendix.

[235] Jack Ewing, *U.S. Growth is Tepid, but It's the Envy of Europe*, N.Y. TIMES (Apr. 28, 2012), http://www.nytimes.com/2012/04/28/business/global/28iht-econ28.html?_r=0.

[236] *See* A. Michael Froomkin, *The Death of Privacy?*, 52 STAN. L. REV. 1461, 1502 (2000).

at an earlier date and restrained some of the most aggressive marketing efforts one commonly sees in the United States.[237] Nevertheless, services like Amazon, Facebook, and Twitter that depend on the exploitation of personal data for their commercial success are hugely popular on both sides of the Atlantic.[238]

The White House and FTC got it about right to the extent that they emphasize education over control. For many, Internet commerce is like visiting a foreign country, where the customs and etiquette are new and often disconcerting. To complicate matters further, the inhabitants of this country are making up their customs as they go along, and the pace of innovation, particularly in the realm of the collection and use of PII, has outpaced the development of shared expectations as to what is acceptable and what is not. A great deal of mischief has been caused by the tendency of companies like Amazon, Facebook, and Twitter to be cagey about their collection and exploitation of PII, leading to surprise and outrage when the facts come to light.[239] To the uninitiated, they seem to have put their feet on the table during dinner without first considering alternative postures or begging the pardon of their dinner mates. In a sense, these companies and their customers are making up a new culture as they go along, and it is not at all surprising that the process causes considerable anxiety and misunderstanding.[240] A guidebook, with information about what to expect in terms of the collection and use of personal information, is important. Many of the recommendations of the FTC's framework and the White House's Bill of Rights can be understood and applauded in this context.

There is, however, a risk of regulatory over-reaction to this collision of cultural expectations. Thanks to the collection of personal information and the assembly of digital identities, consumers obtain better, more personal service than would be possible without it.[241] Consumers can be spared many irrelevant advertisements with which they would be bombarded, commercial television-wise, if the information were not collected, and in the end, it is the exploitation of such information that makes so many free Internet services possible.[242] The assembly of such information both creates enormous new wealth for the companies that compile it and facilitates economic activity for all the other enterprises that take advantage of the information.[243] One does not want to kill the goose laying these golden eggs.[244]

---

[237] *See* Chertoff, *supra* note 213.

[238] *See* Pingdom Team, *The Top Countries on Facebook*, ROYAL PINGDOM (Aug. 12, 2010), http://royal.pingdom.com/2010/08/12/the-top-countries-on-facebook-chart/.

[239] *See, e.g.*, Tony Romm, *Kindle Fire Sparks Lawmaker Privacy Worries*, POLITICO (Oct. 16, 2011, 6:53 PM), http://www.politico.com/news/stories/1011/65978.html.

[240] *See* Natasha Singer, *U.S. is Tightening Web Privacy Rule to Shield Young*, N.Y. TIMES, Sept. 28, 2012, at A1. This report indicates that public complaints regarding misuse of children's information have prompted the FTC to move "to overhaul" the Children's Online Privacy Protection Act in order to expand the scope of information subject to parental consent requirements. *Id.*

[241] William McGeveran, *Disclosure, Endorsement, and Identity in Social Marketing*, 2009 U. ILL. L. REV. 1105, 1114–15 (2009).

[242] *See id.* (discussing Google, which is a free website, and its paid search advertising based on a user's search inquiries or on the content of a user's email exchanges).

[243] Ann Bartow, *Our Data, Ourselves: Privacy, Propertization, and Gender*, 34 U.S.F. L. REV. 633, 647–48 (2000).

[244] The recent about-face by the U.K. Information Commissioner on the subject of cookies exemplifies avoiding the risk of over-reaction. *See* Charles Arthur, *Cookies Law Changed at 11th*

Beyond the economic risk, and from the author's parochial standpoint as an intellectual property lawyer, one must consider whether proposals for the creation of new property rights in personal data can be reconciled with long-established principles of intellectual property law that define the public domain. Without a rich source of raw material in the public domain, the creation of new inventions and works of authorship would be curtailed.[245] Surely no one imagines that an individual should be able to prevent an author from using facts about the individual's life to create a biography, but how does one distinguish this from the assembly of a digital identity by a company like Amazon? The biographer, like Amazon, wants to use the information for her own benefit and to sell the information to third parties to earn a profit. Can one make a reasoned distinction between the two activities? In a sense, Amazon's activity is more benign, because it is quite unlikely to use the information in a way that would offend the individual. Furthermore, if there are "bad facts" about an individual—that he doesn't pay his debts, that he has committed fraud—should he be able to suppress this information because it is his "property"?

This inquiry brings one to an area in which regulation seems appropriate. There are compelling public policy reasons why certain types of information should not inform certain decisions. Race and religious affiliation are perhaps the most obvious examples. Making decisions about the extension of credit, employment, housing, lodging, transport, access to health services, and other universal needs on the basis of race or religion is, and should be, illegal.[246] This is not because an individual owns the fact that she is of a particular race or religion; it is because discrimination on the basis of race or religion is heinous for more general social and historical reasons.[247] On the other hand, it is obvious that some products and services are more appropriately advertised to members of a particular religion or race, and maintaining such information for this purpose provides a valuable service—one probably does not want to try to sell crucifixes to Muslims, and Muslims would probably prefer to be spared crucifix promotions. In other words, it is the use of such information, not its assembly and distribution, that merits legal control.

We come then to a modest proposal: Wherever possible, regulate and provide a remedy for the potential misuse of PII as opposed to its assembly and benign exploitation. Section 604(g) of the FCRA is an example of such regulation.[248] It generally prohibits service providers from obtaining and using medical information

---

Hour to Introduce 'Implied Consent,' THE GUARDIAN (May 25, 2012, 7:22 PM), http://www.guardian.co.uk/technology/2012/may/26/cookies-law-changed-implied-consent. The Information Commissioner had adopted regulations that, on their face, would have required prior consent before any cookie could be placed on an individual's computer. *Id.* This would have made use of the Internet enormously inconvenient, as each visit to a website would have to have been treated as a first visit as if one were required to pretend one did not know someone one had met many times before. *Id.* Under pressure from industry the Commissioner relaxed the regulations to permit Internet interactions to proceed more "normally." *Id.*

[245] A. Samuel Oddi, *The Tragicomedy of the Public Domain in Intellectual Property Law*, 25 HASTINGS COMM. & ENT. L.J. 1, 11 (2002).

[246] *See* U.S. CONST. amend. XIV, § 1; 42 U.S.C. § 3604 (2012) (proscribing housing discrimination specifically).

[247] *See* Brown v. Bd. of Educ., 347 U.S. 483, 492–93 (1954).

[248] 15 U.S.C. § 1681b(g) (2012).

in connection with any determination of the consumer's eligibility, or continued eligibility, for credit.[249] On the other hand, the statute contains no prohibition on creditors obtaining or using medical information for purposes that are not connected to a determination of the consumer's eligibility, or continued eligibility for credit.[250] One can imagine myriad purposes for obtaining such information, not the least of which is the provision of effective medical treatment.

The FCRA takes this a step further in placing the burden on Consumer Reporting Agencies—companies in the business of assembling credit-related information—of policing the limitations on the use of the Consumer Reports they assemble and sell.[251] This approach, which has withstood some forty years of enforcement and development and supports a highly viable industry, could be generalized to include all aggregations of PII that contain information capable of misuse. To use the analogy made earlier in this paper, such aggregations can be considered a modern form of "dangerous instrumentality."[252] Like dynamite, they have many viable purposes, but the person creating and selling these aggregations of PII should bear responsibility for policing their potential for misuse.

This rationale extends as well to laws and regulations placing responsibility on the data aggregators for unauthorized disclosure and for correcting erroneous information upon notice from a consumer. In fairness to legislatures and regulators, many existing and proposed regulations fall into these well-justified categories. One such regulation is the proposed Data Accountability and Trust Act of 2011,[253] which would, among other things, require businesses possessing electronic data to establish security procedures, and to have procedures for verifying and correcting the data.[254] Another example is the proposed Data Security and Breach Notification Act of 2011,[255] which would require security measures and notification in case of breach.[256]

On the other hand, proposed regulation that prohibits entirely the collection of certain types of information, or permits it only with prior consent, seems overbroad.[257] For example, the proposed Geolocation and Privacy Surveillance Act of 2011[258] and proposed Location Privacy Protection Act of 2011[259] would both require prior express consent to the collection of geolocation information.[260] Another example is the proposed BEST PRACTICES Act of 2011,[261] which would among other things,

---

[249] *Id.*

[250] *Id.*

[251] *Id.* § 1681(b).

[252] *See supra* notes 175–179 and accompanying text.

[253] H.R. 1841, 112th Cong. (2011).

[254] *Id.* § 2.

[255] S. 1207, 112th Cong. (2011).

[256] *Id.* § 3.

[257] *See* Clair Cain Miller & Somini Sengupta, *In Mobile World, Tech Giants Scramble to Get Up to Speed*, N.Y. TIMES, Oct. 23, 2012, at A1 ("[J]ust last week, European regulators warned Google to amend its privacy policy that allows it to gather information about people across diverse Google products, from Gmail to YouTube.").

[258] S. 1212, 112th Cong. (2011).

[259] S. 1223, 112th Cong. (2011).

[260] S. 1212 § 2; S. 1223 § 3.

[261] H.R. 611, 112th Cong. (2011).

require prior consent to collect sensitive personal information,[262]. It is not easy to understand how or why a person can legitimately prevent people from knowing his race or that he is walking through a particular mall at a particular time. These facts would be obvious to everyone else in the mall. On the other hand, the use of that information to, for example, rob his home when he is not there, seems legitimately actionable. Again, it is the use, not the information itself, which deserves regulation. Put another way, the appropriate question of public policy concerns use of the information, not its ownership.

CONCLUSION

There is something fundamental at work in the tug of war over the ownership of personal identity. On the one hand, everyone craves a measure of recognition; on the other hand, we morbidly fear exposure. When Brandeis and Warren wrote their classic article on privacy, photography was the new technology, and tabloid journalism was apparently the new business method.[263] They lived in Boston, a large city by nineteenth century standards,[264] and a person living there could probably enjoy a measure of anonymity if he chose to. They saw the new technology and journalism as a threat to that "right to be left alone" and reacted against it with high Victorian umbrage.[265]

One imagines that if they had lived in a smaller place their expectations for privacy would have been very much diminished. In small communities, everyone tends to know quite a lot about everyone else, for better or worse. Some of this knowledge is accurate; much of it is probably exaggerated through gossip and hearsay, but it is an inevitable fact of small-town life.[266] Indeed, it is one of the reasons many people flee small towns when they can.[267] In spite of Brandeis's and Warren's perceived evils of photography and tabloid journalism, a measure of anonymity could be found for many years after 1890 in a big country with big cities, like the United States. Their concern was with what happens behind closed doors in

---

[262] *Id.* § 103.

[263] Warren & Brandeis, *supra* note 82, at 195 ("Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that 'what is whispered in the closet shall be proclaimed from the house-tops.'").

[264] Samantha Barbas, *Saving Privacy from History*, 61 DEPAUL L. REV. 973, 983–844; *see also* JOHN S. BILLINGS, DEP'T OF THE INTERIOR, VITAL STATISTICS OF BOSTON AND PHILADELPHIA COVERING A PERIOD OF SIX YEARS ENDING MAY 31, 1890, at 1 (1895), *available at* www.census.gov/prod/www/abs/decennial/1890.html (reporting Boston's population in 1890 at 448,477).

[265] Warren & Brandeis, *supra* note 82, at 196 ("The press is overstepping in every direction the obvious bounds of propriety and of decency.").

[266] *See* A.G. Sulzberger, *In Small Towns, Gossip Moves to the Web, and Turns Vicious*, N.Y. TIMES, Sept. 20, 2011, at A1 ("In the small towns nestled throughout the Ozarks, people like to say that everybody knows everybody's business—and if they do not, they feel free to offer an educated guess.").

[267] *See id.* (chronicling one woman's strong desire to leave her small town after becoming the subject of a negative and untrue internet posting that caused friends and family to alienate her).

peoples' homes, not the question whether what one does outside of the home is subject to scrutiny.[268]

Now, in the early twenty-first century, privacy law abounds in all the major markets.[269] And the reason is obvious: With the Internet there is no place to hide and no place where one can be anonymous and still engage in commercial life at all. People are somewhat shocked to discover that the Internet has made life in the biggest city as claustrophobic as the smallest of small towns. Just as the butcher, baker, and liquor store owner in a small town will know what consumers eat and drink, will know how much of each, and can gossip freely about consumption habits, and just as the members of a church or synagogue or social club will know an uncomfortable amount about a person's family and its travails, online vendors and social networks will have and may even share a comparable volume of information about a person.[270]

It is not clear that this is an altogether bad thing; on the contrary, as evidenced by Facebook, Twitter, Foursquare, Pinterest, and myriad other social networking sites, people actively seek it.[271] Where, in the past, young people fled small towns to find the anonymity of the big city, today they flee the anonymity of the big city to find recognition in the small towns represented by their friends on networks like Facebook.[272] The difference is that Big Brother, in the person of the collectors of online data, is watching in a way that was never the case in a small town. The same personal information that binds friends becomes more dangerous in the hands of an anonymous corporation or anonymous government agency that can exercise enormous power over the individual.[273]

And so, regulation over the collection and dissemination of such information is both appropriate and inevitable. If successful, it protects against misuse of a person's information, particularly sensitive personal information, and also protects against the dissemination of false or misleading information about that person. Protection against, and remedies for, misuse of personal information should not, however, be confused with ownership of the collections of personal information that comprise identity. This is because, by engaging in commerce or in social media, a person is

---

[268] Warren & Brandeis, *supra* note 82, at 215 ("The general object in view is to protect the privacy of private life, and to whatever degree and in whatever connection a man's life has ceased to be private, before the publication under consideration has been made, to that extent the protection is to be withdrawn.").

[269] *See supra* Part I.B.

[270] *See* FED. TRADE COMM'N, PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE, at iii (1998).

[271] Lim Yung-Hui, *1 Billion Facebook Users on Earth: Are We There Yet?*, FORBES (Sept. 30, 2012, 10:43 PM), http://www.forbes.com/sites/limyunghui/2012/09/30/1-billion-facebook-users-on-earth-are-we-there-yet/ (estimating how long it will take for Facebook to officially surpass one billion users).

[272] *See* Clive Thompson, *I'm So Totally, Digitally Close to You*, N.Y. TIMES, Sept. 7, 2008, at MM42.

[273] *See, e.g.*, *FTC Announces Settlement With Bankrupt Website, Toysmart.com, Regarding Alleged Privacy Policy Violations*, FED. TRADE COMMISSION (July 21, 2000), http://www.ftc.gov/opa/2000/07/toysmart2.htm.

making himself known to others, and others deserve to know whom they are dealing with in both personal and commercial affairs.[274]

Identity and the personal information on which it is built are thus inherently relational in nature. It is the opposite of anonymity, and one cannot have it both ways: You can achieve anonymity by refusing to interact with others, but once you begin to interact, you necessarily lose your anonymity and gain an identity in others' perceptions of you. At that point, your identity is not, and by necessity cannot be, your private possession.

[274] *But see* Assemb. 1844, 2011–12 Leg., Reg. Sess. (Cal. 2012) (prohibiting California employers from requesting their employees' username and password to social media accounts, and making it unlawful to discriminate against those who fail to comply).

APPENDIX

BILLS PENDING IN U.S. CONGRESS AS OF NOVEMBER 1, 2012

Commercial Privacy Bill of Rights Act of 2011 (S. 799)

- Would require commercial entities that use or collect data to implement security measures to protect information and provide users with notice on their collection practices
- Entities must allow users to opt-out of collection of personally identifiable information and unique identifiers and allow users to access and correct data
- Entities may collect only as much information as necessary to process or enforce a transaction
- Authorizes FTC and state AGs to enforce penalties

Do-Not-Track Online Act of 2011 (S. 913)

- Gives the FTC the authority to propose and enforce standards of a Do Not Track mechanism

Do Not Track Me Online Act (H.R. 654)

- Gives the FTC the authority to establish online opt-out mechanisms for users to prohibit collection or use of "covered information"

BEST PRACTICES Act (H.R. 611)

- Advertisers must obtain expressed, written consent to collect "sensitive information," including race, ethnicity, sexual orientation and income
- Requires opt-in consent before a company may disclose information to a third party
- Requires companies collecting personal data to disclose practices and explain options to consumers in timely, easy to understand notices

Consumer Privacy Protection Act of 2011 (H.R. 1528)

- Would require entities to notify consumers that their personally identifiable information may be used for a purpose unrelated to the transaction
- Entities would be required to establish a privacy policy, make it readily available to consumers and notify consumers about changes in their privacy policies
- Entities must give consumers ability to opt out of the sale or disclosure of their information to any organization that is not an information-sharing partner

Geolocational Privacy and Surveillance Act (S. 1212)

- Would prohibit companies from collecting or sharing geolocation information without user consent

Location Privacy Protection Act of 2011 (S. 1223)

- Would require covered entities to offer prior notice and obtain expressed consent from consumers in order to track and collect GPS information

Electronic Communications Privacy Act Amendments Act of 2011 (S. 1011)

- Would update the ECPA to restrict third-party access to GPS information
- Would require authorities to obtain a warrant before accessing an individual's e-mail, digital communications or geolocation information

Data Security and Breach Notification Act of 2011 (S. 1207)

- Requires businesses and NPOs that store personal information to implement reasonable security measures and alert consumers when data has been compromised
- In the event of a breach, affected individuals would be entitled to free credit monitoring for two years

Data Breach Notification Act of 2011 (S. 1408)

- Requires federal agencies and persons engaged in interstate commerce in possession of personally identifiable information to provide notice for any breach of such information

Personal Data Privacy and Security Act of 2011 (S. 1151)

- Would require financial firms, retailers, and federal agencies to guard private information, investigate possible breaches, and notify consumers if their information may have been compromised

Personal Data Protection and Breach Accountability Act of 2011 (S. 1535)

- Would require interstate companies that handle PII on 10,000 or more U.S. persons to provide notice and remedies to consumers in the event of breach
- Holds companies accountable for preventable breaches
- Enhances criminal and civil penalties against unauthorized collection or use of PII

SAFE Data Act (H.R. 2577)

- Would require businesses to notify consumers and the FTC within 48 hours of containing and assessing a breach
- Would entitle affected consumers to two years of free credit monitoring

Digital Accountability and Trust Act (DATA) of 2011 (H.R. 1841)

- Would require FTC to create regulations requiring businesses that own or possess electronic data containing personal information to establish data-security practices and procedures
- Authorizes FTC to require a standard method or methods for destroying obsolete non-electronic data
- Requires information brokers to submit their security policies to the FTC in conjunction with a breach or on FTC request

- Requires FTC to audit security practices of information brokers in the event of a breach
- Requires information brokers to establish procedures to verify the accuracy of information that identifies individuals and to allow consumers to access and correct data