1-1-2007

How and Why We Should Know Less: Information Privacy in Cyberspace

Theodore J. Westbrook
Michigan State University College of Law

HOW AND WHY WE SHOULD KNOW LESS: INFORMATION PRIVACY IN CYBERSPACE

by
Theodore J. Westbrook

Submitted in partial fulfillment of the requirements of the
King Scholar Program
Michigan State University College of Law
under the direction of
Professor Adam Candeub
Spring, 2007

HOW AND WHY WE SHOULD KNOW LESS: INFORMATION PRIVACY IN CYBERSPACE

*Theodore J. Westbrook**

INTRODUCTION 1

I. PRIVACY: OFFLINE AND ONLINE 3

A. What Information Is Being Collected, How, and by Whom? 4

B. The Current Legal Landscape: Eschewing Regulation for Private Ordering 8

A. Economics: What Privacy Means for the Market 13

B. Dignity: Does Self-Determination Justify Restricting Information Flow? 17

III. CHANGING THE RULES: CONTRACTS VERSUS PROPERTY 20

A. A Preliminary Matter: What Makes Information Personal, Private and Protectable? 20

B. Flipping the Switch from Sticky to Teflon: Default Reversal 22

C. A More Complex Approach: Propertization and Inalienabilities 25

CONCLUSION 28

INTRODUCTION

Cyberspace, a globally interconnected web of computer networks, makes unprecedented access to information possible.[1] The architecture of cyberspace, coupled with protocol and common operating methods, have created a system in which personal information about cyberspace users (and other individuals) is collected, aggregated, indexed and stored indefinitely.[2] This is just the beginning, however. Once information is collected, it may be

* Juris Doctor Candidate, Michigan State University College of Law 2007.

[1] *See* CHRISTINE L. BORGMAN, FROM GUTENBERG TO THE GLOBAL INFORMATION INFRASTRUCTURE 1-5 (2000) (discussing the scholarly debate over the changes wrought and to be wrought by cyberspace); *see also* Theodore J. Westbrook, *Owned: Finding a Place for Virtual-World Property*, 2006 MICH. ST. L. REV. 779 (discussing the impact of cyberspace on property law); *see also* Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193, 1195 (1998)

[2] *See* Kang, *supra* note 1, at 1199.

traded in the marketplace or otherwise released, becoming a sort of qualified commons available for an access charge.[3] Information about consumers is an extremely valuable commodity for which companies and individuals are willing to pay a hefty price.[4] The fact that personal information about consumers is easy enough to collect that businesses are willing to pay the asking price speaks to the drastically increased efficiency of data acquisition brought about by the rise of cyberspace. At the same time as personal information becomes increasingly commoditized, available and affordable, information privacy—that is, an individual's ability to control the flow of personal information about him or her[5]—wanes. This paper addresses some of the privacy issues presented by the development of and increased dependency upon cyberspace as a means of communicating and conducting business. Part I provides a backdrop for the discussion, identifying cyberspace privacy issues and their origins and discussing the implications of the current, largely unregulated market for personal information in cyberspace. Part II will discuss the argument for changing the landscape of legal protections for information in cyberspace, including discussions of economics, human dignity and self-determination. Part III will discuss the ways in which the current state may be modified to take better account of both the negative and positive effects of increased flow of personal information in the digital age.

As this paper will discuss and argue, privacy in cyberspace currently exists only to the extent that information is difficult to obtain, not commercially valuable, or tangentially touched upon by generally applicable laws. Because society depends upon cyberspace more and more due to the economic efficiencies of conducting business and other transactions online, the

---

[3] *See* Paul M. Schwartz, *Property, Privacy & Personal Data*, 117 HARV. L. REV. 2056, 2057 (2004); *see also* DANIEL J. SOLOVE, THE DIGITAL PERSON 17-18 (2004) (noting that the demand for information extends beyond consumer preferences to information about consumers themselves).

[4] *See* SOLOVE, *supra* note 3, at 17-18.

[5] *See* ALAN WESTIN, PRIVACY & FREEDOM 7 (1967) (defining "privacy" as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others."); *see also* M. ETHAN KATSH, LAW IN A DIGITAL WORLD 228 (1995) (defining privacy as the power to control what others can come to know about you).

dangers associated with the broad availability of personal information will become increasingly amplified. These dangers include a chilling effect on commercial and other transactions in cyberspace, economic injury and undermining the dignity of persons whose information is compiled, profiled and sold in the marketplace. Scholars have suggested varying solutions to the perceived problem of inadequate cyberspace privacy protections, including propertization of personal information[6] coupled with alienability restrictions and federal legislation that would provide a default privacy policy for online transactions.[7] This paper will explore these two models particularly, and ultimately determine that limited propertization and inalienability of personal information is the preferred method of bringing cyberspace privacy protections into balance. Although restrictive, propertization and qualified inalienability provide strong privacy protection by increasing the transaction costs associated with information trade in cyberspace, thus reintroducing costs that protect individuals from a dangerous level of data aggregation in the non-cyberspace, brick-and-mortar world.

I. PRIVACY: OFFLINE AND ONLINE

"Privacy" admits of a number of definitions in common usage as well as within the law.[8] For example, attorneys may speak of privacy rights with respect to personal or familial decisions or autonomy.[9] This is the type of privacy Justice Douglas discusses in the famous *Griswold v. Connecticut* opinion, in which the Supreme Court found that a constitutional right of privacy prevented the state of Connecticut from legislatively interfering in a married couple's decision to

[6] *See* Schwartz, *supra* note 3, at 2125-26.
[7] *See id.* at 2094; *see also* Kang, *supra* note 1, at 1284-94.
[8] *See* BLACK'S LAW DICTIONARY (8th ed. 2004); *see also* Richard B. Parker, *A Definition of Privacy*, 27 RUTGERS L. REV. 275, 275-76, 277; *see also* Kevin W. Saunders, *Privacy & Social Contract: A Defense of Judicial Activism in Privacy Cases*, 33 ARIZ. L. REV. 811, 814-16 (1991).
[9] *See* Saunders, *supra* note 8, at 815.

use contraceptives.[10] This class of privacy rights obtains primarily, if not exclusively, against government intrusions rather than private intrusions. While "decisional" privacy rights are related to those at stake in a discussion of cyberspace information privacy, a separate class of rights within privacy doctrine applies directly: "informational" privacy.[11] This class of privacy rights is concerned not with the government's power (or lack of power) to interfere in one's personal decisions, but rather with the ability of the individual to be free from the prying eyes of the government and others alike.[12] It is this class of privacy rights that may be defined as an individual's power to control the flow of personal information about him or herself,[13] and which is of primary concern in this paper.

A. What Information Is Being Collected, How, and by Whom?

There are innumerable ways in which cyberspace activities may give rise to information privacy concerns. A familiar example of extensive cyberspace data collection is the system operated by Internet-advertising giant DoubleClick.[14] DoubleClick participates with tens of thousands of web site operators to collect information about site users, analyze the information collected and use it to provide advertisements that are targeted to particular users.[15] In so doing, DoubleClick creates a dossier of information about a particular user, which may include the user's name, address, telephone number, e-mail address, and anything else the user might enter into an input field on a participating website, as well as the user's browsing activities within the

[10] Griswold v. Connecticut, 381 U.S. 479, 485 (1965).
[11] *See* Saunders, *supra* note 8, at 815.
[12] *See id.* at 814-15.
[13] *See* WESTIN, *supra* note 5, at 7; *see also* KATSH, *supra* note 5, at 228.
[14] *See generally* In re DoubleClick Inc. Privacy Litigation, 154 F. Supp. 497 (S.D.N.Y. 2001) (hereinafter "*DoubleClick*").
[15] *See id.* at 502-05.

affiliated web site.[16] Essentially, DoubleClick attempts to gather data and analyze it to create a market-research snapshot of consumer preferences that is keyed to the individual user's Internet Protocol ("IP") address.[17] All of this data acquisition, compilation and analysis takes place without the website user's knowledge or consent.[18]

The DoubleClick "cookie" is just one of innumerable examples of an Internet commonplace known as "spyware" or "adware," computer software whose function is to reside on a particular computer, log any number of different activities in which the computer user is involved, and report this information back to another party.[19] Spyware is a pervasive phenomenon in cyberspace that has gone largely unchecked, partly because data collection using spyware is unquestionably legal under U.S. law if the user "consents" to the installation of the software, e.g., by "agreeing" to the terms of an end-user license agreement packaged with other, useful software.[20] In addition to active gathering of information through software, personal information may also be freely given by cyberspace users, albeit without any expectation that this information may be retained, processed into a searchable database or dossier, and possibly given away, traded or sold.[21] For example, a cyberspace user making an online purchase may be required to provide answers to a series of questions before the transaction may be completed. These questions could include not only information that is functionally necessary to complete the

---

[16] *See id.* at 504.
[17] *See id.*
[18] *See id*. at 502-05.
[19] *See* Wayne R. Barnes, *Rethinking Spyware: Questioning the Propriety of Contractual Consent to Online Surveillance*, 39 U.C. DAVIS L. REV. 1545, 1547, 1552-56 (2006) (discussing definitions of "spyware" and "adware" and how these programs are used).
[20] *See id.* at 1594.
[21] *See* Kang, *supra* note 1, at 1223-29 (walking through a typical cyberspace purchase, in which the seller may collect not only data that is necessary to complete the transaction, but other data as well); *see also* LAWRENCE LESSIG, CODE 143-44 (1999) (arguing that there is a real distinction between what may be monitored and what may be searched, and that the latter is far more problematic from the standpoint of cyberspace privacy). An entirely separate phenomenon, demonstrated by MySpace, Facebook, Friendster and many other web services, is the growing popularity of social networking services in cyberspace. Users of these services sometimes post to their "profiles" or "pictures" pages surprisingly intimate and personal information, which then becomes searchable by other members of the network.

transaction, such as the purchaser's name, shipping address and payment information, but also other information the seller wishes to obtain from the buyer.[22] This is essentially the online equivalent of brick-and-mortar stores asking customers at the register for their home zip codes or phone numbers, even when the customer pays in cash.[23] Once this information is released, the consumer has effectively waived all means of corralling it.

The architecture of cyberspace is, to an extent, responsible for the distinctions between a real-world transaction and a similar transaction in cyberspace.[24] There is no lack of opportunities to gather information in the real world; someone shopping in a mall would not be surprised at the fact that she may be readily observed by passersby. A variety of information could be gleaned from such observation, including physical characteristics of the person, the clothes she is wearing, at which stores she has been making purchases and so forth. This information could easily be stored, as well, using primitive technology such as a pen and notebook. However, if she uses cash, there is no identifiable record of her purchasing habits over the long term, and most of the information that may be gathered through casual observation is not necessarily linked to her identity. That is, the casual observer does not know her name, where she lives, her phone number, her social security number or anything beyond the superficial. Cyberspace transactions may differ in most or all of these respects, since physical presence at the shopping site is eschewed in cyberspace transactions in favor of code. Every bit of one's "presence" in cyberspace consists of data that is easily moved and duplicated as well as easily, inexpensively and often automatically stored.[25] Such detailed record-keeping in the

[22] *See* SOLOVE, *supra* note 3, at 22-26.
[23] *See Privacy: Don't Give Away Your Phone Number at the Store*, LIFEHACKER, http://lifehacker.com/software/privacy/dont-give-your-phone-number-away-at-the-store-140530.php.
[24] *See* LESSIG, *supra* note 21, at 142 ("Here the code has already upset a traditional balance. It has already changed the control that individuals have over facts about their private lives. The question now is: Could code re-create something of a traditional balance?").
[25] *See* Kang, *supra* note 1, at 1226-27.

brick-and-mortar world would be not only intrusive and expensive; it would likely be highly disconcerting to the average weekend mall patron. On the other hand, the brick-and-mortar world is not free from data aggregators; indeed, technological innovations as well as novel business practices have combined to make data aggregation economically feasible under the right circumstances. For example, it has become fairly standard for supermarkets to track the purchases of their patrons using "rewards" cards that link purchases to the shopper's identity, operate a database that accomplishes a similar end through credit card tracking, or utilize RFID technology that has the potential to gather and store even more information about consumers.[26] At the current stage, however, data aggregation such as that present in some supermarket transactions is limited in scope outside of cyberspace, whereas it is virtually limitless within cyberspace.

A key distinction between most brick-and-mortar observation (aside from the outliers mentioned above) and the data collection and aggregation that is common in cyberspace is the cost. In the non-cyberspace world, the cost of obtaining, storing, indexing and analyzing data is typically substantially higher than in cyberspace. In the shopping mall example, sending agents to the mall to follow patrons around, identify them and track their purchases would be incredibly costly. The mall, unlike cyberspace, does not have the tools of data collection and aggregation built into its infrastructure. In order to present an analogous data collection situation to cyberspace transactions, the mall would have to require patrons to identify themselves upon entry, swipe an identification card at the entrance of every store, swipe it again upon making any purchase and again upon leaving. Store clerks would have to keep records of which items each

[26] *See generally* Serena G. Stein, *Where Will Consumers Find Protection from RFIDs? A Case for Federal Legislation*, 2007 DUKE L. & TECH. REV. 3 (2007). For a listing of grocery store chains that utilize such data aggregation technology and methods, see C.A.S.P.I.A.N. – Consumers Against Supermarket Privacy Invasion and Numbering, http://www.nocards.org.

patron browsed or showed interest in. Further, the identification swiped would have to reveal additional information, such as the patron's address and phone number. Only under these extraordinary circumstances would a brick-and-mortar mall approach the data-collecting capacity of a *typical* cyberspace transaction.

B. The Current Legal Landscape: Eschewing Regulation for Private Ordering

Cyberspace information privacy with respect to private parties (as opposed to the government) is essentially unregulated under United States law.[27] Although data privacy is protected to some extent by statutory schemes such as the Electronic Communications Privacy Act ("ECPA"),[28] certain provisions of that act tend to negate its effects on the realm of cyberspace transactions.[29] The ECPA prohibits acquisition of certain forms of data by interception; however, it is a defense to a private action under the ECPA that the plaintiff consented to the gathering of the information.[30] This is significant because much of the personal information that finds its way into cyberspace was placed there by users themselves, during the course of online transactions. It may be difficult for such users to argue that the information was obtained without their consent, since such consent seems clearly implied by the fact that the information was voluntarily given.[31] The failing of the ECPA is that consent to the *collection* of the information at issue is not the most relevant criterion to information privacy. Rather, the crucial inquiry is whether the individual to whom the information pertains consents to the *use* to which that information is to be put, both during and after the information transaction. The ECPA

[27] *See* Kang, *supra* note 1, at 1230.
[28] Electronic Communications Privacy Act ("ECPA"), 18 U.S.C. §§ 2510-22; 2701-10.
[29] *See id.*
[30] *Id.* § 2701(c).
[31] *See* In re DoubleClick Inc. Privacy Litigation, 154 F. Supp. 2d 497, 507-11 (S.D.N.Y. 2001) (finding the ECPA inapplicable because users of affiliated websites voluntarily submitted information to affiliates and thus consented to the gathering of information).

does not touch on information use; it focuses purely on the circumstances under which information is obtained.[32]

Common law or statutory tort liability for invasion of privacy is a relatively old tradition in the United States, dating back to *The Right to Privacy*, a highly influential article written by Samuel Warren and Louis Brandeis, discussing the lack of privacy protections brought about by the advent of yellow journalism.[33] Largely in response to this article, courts in the ensuing decades created privacy torts to address the parade of horribles described by Warren and Brandeis, and which collectively became known as "invasion of privacy" torts.[34] Although the title of these torts might seem promising with regard to cyberspace information privacy, in fact they miss the mark substantially. In order to prevail on a typical invasion claim, a plaintiff must show that the intrusion into his personal, private affairs "would be highly offensive to a reasonable person."[35] In isolation, gathering a single piece of personal information about an individual is unlikely to meet the "highly offensive" threshold. It is not the collection of the information that is problematic in cyberspace; it is the aggregation of all of these pieces of information into a single, searchable and identifiable unit that poses real problems,[36] in addition to the possibility of unauthorized downstream information transfers and eventual misuse of sensitive data. Existing privacy torts fall flat in this regard. Again, as with the ECPA, the emphasis in privacy torts seems to be on how information is *collected*, not how it is ultimately *used*.

---

[32] *See* ECPA, 18 U.S.C. §§ 2701-10.
[33] Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).
[34] *See* Irwin R. Kramer, *The Birth of Privacy Law: A Century Since Warren and Brandeis*, 39 CATH. U. L. REV. 703, 704 (1990).
[35] *See* RESTATEMENT 2D OF TORTS § 652B (1976).
[36] *See* Daniel J. Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy*, 53 STAN. L. REV. 1393, 1432 (2001).

Information privacy in cyberspace is only tangentially regulated under existing U.S. law. Unlike the privacy protections in place under European law, there is no requirement under U.S. law that parties collecting information specify what uses may be made of that information once gathered.[37] The Constitution itself is largely irrelevant to data privacy in cyberspace, since constitutional guarantees apply as against the state and not against private parties; further, the extent of the Constitution's protection of data privacy is particularly unclear even as against the state.[38] There are numerous general federal and state statutes that touch lightly on issues of cyberspace privacy, such as the aforementioned federal ECPA, [39] Fair Credit Reporting Act, [40] Family Educational Rights and Privacy Act,[41] Cable Communications Privacy Act,[42] the Gramm-Leach-Bliley Act[43] and a number of state-law analogues to those federal statutes.[44] While these statutes provide some protection in the context of cyberspace transactions that fall within their ambits, they do not substantially regulate data privacy in typical cyberspace transactions, such as online purchases, web browsing and search engine use. Instead, much of the "regulation" of cyberspace information practices comes in the form of private ordering. In other words, to the extent that it exists at all, regulation of cyberspace information privacy comes in the form of contracts.

---

[37] *See* PAUL M. SCHWARTZ & JOEL R. REIDENBERG, DATA PRIVACY LAW § 10-2(a)(1), 241 (1996) (noting that, unlike European law, U.S. law does not require specification of purposes for data collection).
[38] *See* Kang, *supra* note 2, at 1230 n. 157 ("A right to information privacy has not been clearly established as a matter of federal constitutional law."). This paper is premised on an assumption that the state of data privacy in cyberspace is affected more by private actions and market forces than by government intrusions; thus, statutory structures that only effectively limit the government's access to records in cyberspace are largely irrelevant or, at the very least, not sufficient to support cyberspace data privacy in its entirety.
[39] Electronic Communications Privacy Act of 1986, 18 U.S.C. §§ 2510-2522, 2701-2709 (1988 & Supp. 1994).
[40] Fair Credit Reporting Act of 1970, 15 U.S.C. §1681 (1988).
[41] Family Educational Rights & Privacy Act of 1988, 20 U.S.C. §§ 1221 (1988).
[42] Cable Communications Policy Act of 1984, 47 U.S.C. § 551 (1988).
[43] Gramm-Leach-Bliley Act, Pub. L. No. 106-102, §§ 501-527, 113 Stat. 1338, 1436-50 (1999) (codified at 15 U.S.C. §§ 6821-6827 (2000)).
[44] *See* Kang, *supra* note 1, at 1232; *see also* SCHWARTZ & REIDENBERG, *supra* note 37, at 131 (noting that most states do not have omnibus data privacy protection statutes, and only 13 states have passed laws analogous to the federal Privacy Act but applying to state rather than federal actors).

Cyberspace originally functioned as a sort of commons, a place wherein regulation was unknown and, many thought, unknowable.[45] The anarchic nature of cyberspace has slowly morphed to take account of generally applicable laws; for instance, there is no longer much room to argue that one may make illegal copies of movies or music files available for others to download via the Internet—at least not with impunity.[46] At the same time, however, much has been left to contracts. For instance, the ECPA, which prohibits the interception of certain types of data, may be conveniently contracted around by having the user (whose information is to be gathered) consent to the gathering of his or her personal information via a "click-wrap" style agreement, whereby the consumer assents to a set of on-screen terms of use, an end-user license agreement ("EULA") or another type of contract by clicking a virtual button stating "I Agree."[47] Probably most software users, including most cyberspace users, have encountered such click-wrap agreements, which may contain lengthy disclaimers of responsibility as well as laying out the privacy policy of the software or service provider with respect to personal data collected during the transaction.[48] Although empirical data are scarce on this point, it may be safe to assume that most users do not read such agreements, but instead assume that the terms are proper and click "I Agree." In so doing, they may be giving up any rights to control the flow of

[45] *See* Lawrence Lessig, *Foreword* to *Cyberspace & Privacy Symposium* (Feb. 6, 2000), 52 STAN. L. REV. 987, 995 (2000) (describing the generally anarchic nature of cyberspace at its inception).
[46] *See*, *e.g.* Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd., 545 U.S. 913 (2005) (finding peer-to-peer file-sharing network contributorily liable for copyright infringement of users); BMG Music v. Gonzalez, 430 F.3d 888 (7th Cir. 2005) (finding user of Internet file-sharing service liable for copyright infringement after downloading illegally copied music files).
[47] Several courts have upheld "click-wrap" agreements as legally binding. *See* Specht v. Netscape Commc'ns Corp., 306 F.3d 17, 23 n.4 (2d Cir. 2002) (citing a number of courts so holding). Additionally, the National Conference of Commissioners on Uniform State Laws has proposed the Uniform Computer Information Transactions Act, section 112 of which would provide for the enforceability of click-wrap style agreements in their most common forms. *See* RAYMOND S. R. KU ET AL., CYBERSPACE LAW 651-53 (2002). *See generally* Margaret Jane Radin, *Humans, Computers & Binding Commitment*, 75 IND. L.J. 1125 (2000) (discussing new forms of contracts and licensing agreements arising in the context of the World Wide Web).
[48] *See* Barnes, *supra* note 19, at 1594-98.

personal information gathered during the transaction, effectively giving the information-gathering party all power and control over such information.

This explanation of the way data is routinely treated in cyberspace may seem abstract and attenuated from reality; however, the real-world implications of increased availability and flow of personal information in cyberspace are in fact rather staggering. Perhaps the most pervasive data-collection tool in cyberspace, spyware can facilitate the release of incredibly detailed and private information concerning the unsuspecting host-user.[49] This information can include financial information, records of the user's online purchases, as well as information related to the user's politics, religion, family and health.[50] Financial information, including bank account numbers and balances, could be obtained through monitoring of the user's online banking activity. Likewise, credit card numbers and consumer preferences and purchasing habits may be discovered through monitoring of the user's activity in the cyberspace marketplace. An accurate log of a user's simple web browsing habits could reveal any number of sensitive pieces of information; for example, a user who spends a great deal of time browsing websites concerning a particular medical condition (e.g. mesothelioma) or political issue (e.g. border security) may be associated with these topics in the dossier of an information-gathering company. Again, with no particular limits as to how this information may be used once gathered, an individual could be subject to strategic uses of information ranging from targeted direct-mail advertising to identity theft to political intimidation.

[49] *See* Barnes, *supra* note 19, at 1560-61.
[50] All of this may be accomplished through the use of key-logging software. *See id.* at 1561.

II. PRIVACY, ECONOMICS AND DIGNITY: THE CASE FOR OVERHAUL

Part I introduced some of the basics and implications of cyberspace information privacy as between private—often transacting or contracting—parties, as well as providing an overview of the law (or lack thereof) related to cyberspace privacy issues. Part II will discuss the arguments for changing the landscape of cyberspace information privacy regulation, as well as arguments for leaving it largely unregulated. Particularly, this discussion will take account of two distinct but related arguments for cyberspace privacy reform: the economic implications of information privacy, and information privacy from the standpoint of human dignity. Each of these arguments provides a strong basis for altering the current cyberspace environment to facilitate enhanced data privacy.

A. Economics: What Privacy Means for the Market

Information privacy has its detractors as well as its champions among commentators with economic leanings.[51] In part, the debate boils down to a simple dichotomy: does the free flow of personal information about consumers *improve* market efficiency by allowing resources to be spent on precisely targeted marketing efforts rather than a scattergun approach;[52] or does the free flow of personal information *undermine* market efficiency by scaring consumers away from cyberspace activities and transactions?[53] Additional questions of market inefficiency center on whether market prices for personal information are inefficiently low because of a severe

[51] *See generally* Richard S. Murphy, *Property Rights in Personal Information: An Economic Defense of Privacy*, 84 GEO. L.J. 2381 (1996) (arguing that while disclosure of personal information benefits the market by improving the targeting of products and services, privacy benefits the market by encouraging consumers not to shy away from making bargains). *See also* Steven A. Bibas, *A Contractual Approach to Data Privacy*, 17 HARV. J.L. & PUB. POL'Y 591, 604-05 (1994) (arguing that consumer preferences about privacy affect prices).
[52] *See* Bibas, *supra* note 51, at 604-05.
[53] *See* David H. Freedman, *Why Privacy Won't Matter*, NEWSWEEK INT'L April 3, 2006; *see also* David N. Schachter, *Cyberspace Privacy Battle is in High Gear*, DENVER BUSINESS JOURNAL, May 25, 2001, at 31A (stating that "the easiest and cheapest privacy protection is still the most effective as well: just don't log on.").

asymmetry of information as between cyberspace users and data collectors. Perhaps unsurprisingly, database industry advocates—as well as some presumably less biased commentators—argue that the market is already accounting for the costs and benefits associated with the collection and distribution of personal information, and thus that the current legal landscape of minimal regulation is fully adequate.[54] However, this argument rests on a failure to account for a number of important economic complications, including the asymmetry of information in favor of the data collector, an almost complete lack of opportunity for the subject to alter the bargain that results in releasing information, and other phenomena that can be handily summarized in economic terms as "transaction costs."[55]

The uncertain state of privacy in cyberspace is not lost on users. In fact, there are some indications that apprehensiveness about the privacy of personal information has had a serious chilling effect on commerce and other activities in cyberspace, as those most concerned about privacy find greater peace of mind in refraining from undertaking such activities.[56] The extent of the chilling effect has not been accurately measured, nor is it likely to be accurately measured; however, it is clear enough that if consumers simply choose to forego cyberspace and the economic efficiencies it does often provide, the short-term economic efficiencies created by the free flow of personal information will be more than offset. Further, it seems very likely that if more consumers were better informed about how their personal information might make it onto a dossier or otherwise be disclosed, more consumers would in fact severely limit their cyberspace activities. This raises the question whether it is the place of law and government to protect

[54] *See* Solove, *supra* note 36, at 1447 (citing *Privacy in Commercial World*, 106th Cong. (2001) (statement of Paul H. Rubin, Professor of Law and Economics, Emory University School of Law), available at http://www.house.gov/commerce/hearings/0301200143/Rubin66.htm)); *see also* Bibas, *supra* note 51, at 604-05.
[55] *See* Kang, *supra* note 1, at 1248.
[56] *See* Charles Raab, *Regulatory Provisions for Privacy Protection*, in THE GLASS CONSUMER 45 (Susanne Lace ed., 2005).

individuals from their own ignorance. Would restrictions on the flow of personal information in cyberspace constitute unacceptable government paternalism? Free-market proponents would argue that individuals should be free to contract as they see fit and to give or trade away their personal information if they choose to do so.[57] Again, this argument ignores the fact that individuals do not typically understand the implications of releasing information in cyberspace, instead assuming perfect information.

Personal information is chronically undervalued by consumers. Users are often willing to give up such information to data collectors in exchange for little or nothing of value. This is unusual considering the value placed upon indexed personal information for the purposes of, e.g., targeted marketing, and probably reflects one or both of two misunderstandings: (1) consumers do not understand that information about them can be used in plenary fashion once it is initially disclosed, making the initial information transaction relatively more valuable; and (2) consumers assume that adequate legal protections are already in place with respect to permissible uses of their personal information. Each of these misunderstandings has the effect of reducing the price of data collection by encouraging consumers to demand less in exchange for the data. In this circumstance, data collectors are the beneficiaries of a giant windfall while consumers are deprived of the fair market value of their information both in the initial information transaction and in downstream transfers, for which they are not compensated at all.

Thus, while the current dearth of regulation in cyberspace information privacy arguably creates economic efficiencies by allowing freer flow of information and faster, cheaper transactions, the benefits of these efficiencies run in only one direction and are not shared by consumers. This situation is brought about by information asymmetry which, if resolved, would work to make cyberspace users more skeptical of cyberspace transactions. The natural results of

[57] *See* SOLOVE, *supra* note 3, at 90-91.

this skepticism would be (1) increased transaction costs because of a chilling effect on cyberspace transactions in general; and (2) further increased transaction costs incurred by cyberspace users who are willing to take the extensive precautions necessary to limit information disclosure. While methods do exist for consumers to protect themselves from data aggregation, these methods are neither perfect nor convenient. Anonymous web browsing, which allows users to mask their IP addresses to avoid certain types of data logging, [58] introduces delays and other expenses as well as limited functionality, and cannot protect users against all forms of data collection. Likewise, use of spywyare-removal software[59] is imperfect because the software will catch and eliminate only a fraction of the privacy threats that may be present. It also not inconceivable that anonymous web browsing services and spyware removal software could themselves incorporate data-logging technology, thus defeating their purpose as privacy protections and further undermining the individual's ability to shoulder the burden of protecting his or her own privacy.

Transaction costs in the market for personal information in cyberspace are inefficiently low on the side of data aggregators as a result of the prevailing underregulated environment, resulting in a kind of overproduction of personal data. Moreover, the current data market is unstable in that it appears to be founded on the ignorance of the initial sellers of a key input: consumers. Thus, privacy protections that establish higher transaction costs in the cyberspace information market with respect to sensitive information about individuals act not only as a

[58] *See*, *e.g.* The Cloak, http://www.the-cloak.com (offering free anonymous web browsing service); Anonymizer, http://www.anonymizer.com (offering a similar service). These services are available in low-bandwidth mode free of charge, or for a fee if the user requires enhanced bandwidth.

[59] For an example of such software, see http://www.lavasoft.com. Ad-Aware is a spyware removal tool offered by software developer Lavasoft. Although it is also offered in free and pay versions, using the software imposes burdens on the user and his or her computer in other ways, including time spent setting up and maintaining the software and its database, and time and lost productivity while letting the software run periodically.

safeguard to protect consumer interests, but also to stabilize the market for such information and to prevent the market from failing once better information is available to consumers.

B. Dignity: Does Self-Determination Justify Restricting Information Flow?

The economics arguments may fall upon a number of deaf ears as missing the point of a privacy discussion, ignoring crucial facts or simply failing to account for the moral and human aspects of information privacy. If we dismiss economics as an accurate way to approach privacy issues,[60] there remains a normative approach centered on dignity rather than the market.[61] Although this approach seems somewhat ill-defined from the standpoint of U.S. law, it already factors prominently in European data protection laws.[62] Information privacy as dignity is the concept that the injury to an individual resulting from misappropriation or misuse of personal information about him or her is not an economic injury, but rather an injury to the individual's personhood and right of self-determination, which could collectively be called "dignity."[63] Although certainly more of an emotional argument than the economic approach, the argument to dignity is powerful in that it is intuitively correct and gives a defensible moral basis for protecting information privacy rights in cyberspace. Moreover, it is rooted in the very same fundamental values expressed by Warren and Brandeis in the article that launched a privacy

[60] *See* A. Mitchell Polinsky, Comment, *Economic Analysis As a Potentially Defective Product: A Buyer's Guide to Posner's Economic Analysis of Law*, 87 HARV. L. REV. 1655, 1670 (1974) (arguing that economic analysis of law is skewed by the assignment of property rights and liability rules).
[61] *See* Edward J. Bloustein, *Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser*, 39 N.Y.U. L. REV. 962, 973-74 (1964).
[62] *See* Corey A. Ciocchetti, *E-Commerce and Information Privacy: Privacy Policies as Personal Information Protectors*, 44 AM. BUS. L. J. 55, 66-67 (2007) (citing Parliament and Council Directive 95/46EC 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), also known as "EU Privacy Directive").
[63] *See* Bloustein, *supra* note 61, at 973-74 ("A man whose … conversation may be overheard at the will of another, whose marital and familial intimacies may be overseen at the will of another, is less of a man, has less human dignity, on that account.").

revolution in the United States: the right "to be let alone,"[64] and the right to protect one's "inviolate personality."[65]

Under the dignity model, the right to privacy is an inviolate right that "protects the individual's interest in becoming, being, and remaining a person."[66] This vaguely Hegelian construction of privacy, which seems likewise somewhat impenetrable, takes on great meaning in the context of appropriate examples. One such example is the practice of "outing" gays and lesbians in efforts to cause humiliation and to subject individuals to the moral condemnation and other social stigmatization that may accompany publicizing this information.[67] Unregulated cyberspace provides incredibly powerful tools that could be used to "out" gay and lesbian cyberspace users more quickly, easily and publicly than ever before. In a regulatory structure in which individuals have no say over the flow of personal information about them, human dignity is continually at risk from this and similar threats; e.g., disclosure of information such as health, alcohol and drug use, sexual offense victim status, abortion patient status or any other potentially damaging and deeply personal information.[68]

Similar examples of misuse of sensitive information are innumerable in character. An individual's medical history—which may be more or less sensitive depending on its contents—could be disclosed to anyone by a data collector in the absence of any protective agreement. This disclosure could lead to unacceptable consequences ranging from improper marketing of

---

[64] *See* Warren & Brandeis, *supra* note 33, at 195
[65] *See id.* at 205, 211.
[66] Jeffrey H. Reiman, *Privacy, Intimacy and Personhood*, in PHILOSOPHICAL DIMENSIONS OF PRIVACY 300, 314 (Ferdinand David Shoeman ed., 1984). As support for this notion, Reiman discusses the practice in prisons of total deprivation of privacy, in an effort to mortify the inmate's sense of self and individuality. *See id.* at 311.
[67] *Cf.* PAUL FAIRFIELD, PUBLIC/PRIVATE 47 (2005) (arguing that this and other practices are undertaken to, and in fact, injure the individual's sense of dignity, self-determination and power in general.)
[68] *See* Daniel J. Solove, *The Virtues of Knowing Less: Justifying Privacy Protections Against Disclosure*, 53 DUKE L.J. 967, 972 (2003) (identifying these areas as those in which states have been willing to regulate information in non-cyberspace contexts).

pharmaceuticals and other "curative" products[69] to the disclosure of a list of abortion clinic patients. Even if these disclosures do not result in tangible, physical harms to the individuals described by the information, the fact that the individual has been deprived of the ability to choose for him or herself whether such information becomes widely known is a blow to the individual's right of self-determination.

Although the argument to dignity might seem to justify bolstering legal protections of information privacy on entirely moral grounds, proponents of economic theory might argue otherwise. Even accepting the premise that personal information disclosure can negatively affect human dignity, economists might argue that an individual could place a value on his or her own dignity in just the same way as any other commodity in the marketplace, and that a suitable equilibrium that accounts for dignity could be reached. This equilibrium could reduce or eliminate the need for a restrictive regulatory structure to govern information privacy in cyberspace. That argument, however, runs into the same difficulties as does the economic argument to retain the status quo of minimal regulatory interference in the cyberspace information trade. That is, a substantial asymmetry of information makes valuing personal information, and likewise the impact that disclosing personal information can have on dignity, difficult if not impossible. The economic and dignity arguments for increased regulation of cyberspace information privacy are intertwined in that both militate towards greater control of information by individuals that comes, in part, through increased knowledge about the possible uses of information released and collected in cyberspace.

[69] *See* SOLOVE, *supra* note 3, at 22-23 (noting that a data collector called Hippo Direct "markets lists of people suffering from 'medical maladies.' such as constipation, cancer, diabetes, heart disease, impotence, migraines, enlarged prostate and more.").

III. CHANGING THE RULES: CONTRACTS VERSUS PROPERTY

In Part II, this paper has discussed three lines of argument that may militate in favor of disturbing the current trend of minimal regulation of information privacy in cyberspace, namely economics, dignity and self-determination. This Part returns to the essential business of the paper: parsing out the most viable alternatives to the current trend, and arguing for implementing the best of these alternatives. Particularly, the discussion will focus on two alternatives to the current market-based approach. The first of these alternatives, which I will call "default reversal," is itself a market-based approach, which simply changes the default privacy policy from one that provides no restrictions to data collection and disclosure, to a policy of collecting and processing information in only "functionally necessary" ways.[70] This default could be overcome easily by a contrary contract between the parties to a transaction. The second alternative consists of rethinking the nature of personal information, essentially changing the status of information from a commons to private property, while providing certain restrictions on alienability to account for various problems, including transaction costs.[71]

A. A Preliminary Matter: What Makes Information Personal, Private and Protectable?

It would be nonsensical to treat every type of information identifiable to an individual as legally protected. No benefit would derive from a rule creating privacy rights with regard to common knowledge or information that is a matter of public record, and the concomitant costs could be enormous. However, it is difficult to define the precise distinction between information that is private or personal and information that ought to be left unprotected.[72] The difficulty of

[70] *See* Kang, *supra* note 1, at 1249.
[71] *See* Schwartz, *supra* note 3, at 2094-96.
[72] *See* Kang, *supra* note 1, at 1287, 1287 n. 370 (discussing the difficulty of determining what types of information qualify as "sensitive").

defining such a distinction has led some scholars to abandon the idea and instead propose data protection regardless of the type of data.[73] Attempts to protect information privacy without distinguishing between sensitive and non-sensitive information are bound to fail on account of their overbreadth, however.

It is important to note that a set of data does not pose particular privacy problems exclusively by virtue of containing individual pieces of information that are themselves personal or private, although a data set containing such pieces of information is likely to pose some problems. Determining whether an individual piece of information is sensitive is very difficult in all but the easiest cases. For example, it is easy to see how one's medical history, financial information and sexuality could be considered private and sensitive, while one's date of birth or eye color should not be considered sensitive. Many cases fall somewhere on the border between those two easy cases, particularly when aggregated data is accounted for. For example, it would be hard to argue that public-record information such as the names and ages of one's children is personal information; however, once that information is aggregated with additional information, such as the children's address and the parents' normal working hours, it arguably takes on personal or private status. This example demonstrates why the critical aspect of data that implicates privacy concerns is aggregation,[74] or how much and which types of information are available at the same time, by the same party or from the same source.

That a data set contains individual pieces of information that are considered sensitive or personal cannot be the *sine qua non* of protectability. The distinction between personal information and non-personal information instead ought to account for the increased impact and

[73] *See id.*
[74] *See* SOLOVE, *supra* note 3, at 87-88 (arguing that aggregation, which can take place over a number of different, smaller information transactions, causes much more powerful collections of data to be amassed while simultaneously hiding the value of individual pieces of information disclosed by the individual user).

value of aggregated, personally identifiable information. I propose that a set of data ought to be considered personal—and thus protectable—if, taken as a whole, it reflects personally identifiable information that a reasonable person would choose not to disclose to unknown recipients. Although this formulation presents a flexible standard rather than a rigid rule, it is advantageous in that it both recognizes the increased impact of aggregated data, as well as alleviates the need to compose an exhaustive list of criteria for a single piece of information to qualify as personal, private or protected.

B. Flipping the Switch from Sticky to Teflon: Default Reversal

As explained in Part I above, the default rule in cyberspace information transactions is, essentially, no rule at all. That is, once information is obtained by a collecting party, that information is available for plenary, relatively unrestricted use in the marketplace or otherwise.[75] This default rule is a double-edged sword in that although it allows a great deal of flexibility in the market for information and thus improved efficiencies in marketing and other services, it also fails to protect individuals from potentially abusive uses of their personal information.[76] This situation not only threatens human dignity, but also calls into question the economic efficiencies of the default rule, since it may have a chilling effect on cyberspace transactions.[77] One alternative to the current dearth of regulation is a simple-sounding change in the default rule from "plenary use" to "functionally necessary use."[78]

[75] *See id.* at 1249. This assumes that the information was obtained lawfully and not in contravention of any existing, generally applicable law such as the ECPA, which prohibits certain types of data interception.
[76] *See* discussion, *supra* Part II.A.
[77] *See* discussion *supra* Parts II.A and II.B.
[78] *See* Kang, *supra* note 1, at 1249-59.

"Functionally necessary use" signifies uses of information that are required to carry out the transaction in which the information was collected.[79] For example, if a cyberspace user were to engage in an online purchase with a seller, the seller would be permitted to make use of the information submitted in connection with the purchase, but only insofar as that information were necessary to complete the transaction. The individual's address information, for example, could be transmitted to the courier for the purposes of delivery, but could not be sold to another company for use in a marketing database. A functionally necessary default rule could, however, be altered by contract between the individual and the data collector,[80] such that the purchaser in our example could agree that his information be made available to marketing affiliates of the seller.

As Professor Kang explains, some legal rules that are alterable by contract are "sticky," meaning the default rule is difficult to change and is thus likely to become the only way of doing things.[81] Other legal rules are "Teflon" or non-stick, meaning that it is easy for contracting parties to "flip" the default rule, thus allowing a greater variety and degree of customizability in the rule as applied.[82] A default rule of plenary use is "sticky" because data collectors probably will not be willing to negotiate with cyberspace users concerning the terms of personal information use. Further, transaction costs for the user are prohibitive because of the costs associated with (1) finding out who the potential information collectors and users are; (2) contacting them; and (3) negotiating with them to limit their use of personal information about the user.[83] On the other hand, a default rule of strictly functionally necessary use is "Teflon"

[79] *See id.* at 1249.
[80] *See id.* at 1250.
[81] *See id.* at 1256-58.
[82] *See id.* at 1258.
[83] *See id.* at 1253-54. Professor Kang also argues that there is a serious collective action problem at work in "flipping" the default of plenary use. *Id.*

because none of the prohibitive transaction costs of the plenary use default apply.[84] If the potential data collector aims to make use of information beyond what is functionally necessary, it will have to convince the user to agree to such use; this could easily be accomplished through, e.g., a "click-wrap" agreement specifying the terms of use.

A functionally necessary default rule regarding personal data in cyberspace could affect some positive change in that, under such a regime, the individual's consent would virtually always be required before personal information about him or her could be used in a potentially harmful or obnoxious way. This is particularly true with regard to marketing data collectors such as DoubleClick.[85] If DoubleClick-affiliated websites wished to share personal information about their users, they would have to find a way to contract around the functionally necessary default rule.[86] The default switch is not a perfect solution, however. Many cyberspace information-gathering entities already present the user with a privacy policy, to which the user must agree before being allowed to access the desired service.[87] These policies, which may very well be ignored by most cyberspace users, are typically long, written in dense legalese and either overwhelming or simply indecipherable to laypersons.[88] The "bargain" represented by such privacy contracts may be nearly as "sticky" as the plenary use default rule, since the user is typically unable to negotiate a different privacy policy, and must instead choose either to assent to the terms presented—no matter how repugnant or confusing—or to instead forego the transaction in its entirety. It is likely that the main effect of switching the default rules from plenary use to functionally necessary use would be the proliferation of "click-wrap" agreements

[84] *See id.* at 1256-57.
[85] *See* discussion *supra* Part I.A.
[86] This is, of course, assuming that the entire function of the information transaction was not to facilitate targeted advertisements. If that were in fact the purpose of the transaction, a strong argument could be made that the information sharing were functionally necessary to further that purpose.
[87] *See* Barnes, *supra* note 19, at 1594-98.
[88] *See id.*

ad absurdum, to the point where users must effectively decide whether to trust a marketplace full of hungry data collectors by agreeing to every privacy policy without question or investigation, or to simply refrain from ever logging in. Both of these situations are highly problematic; the former because it leaves the consumer with as little control as possible over the information gathered about him or her while still demonstrating the same economic inefficiencies as the current antiregulatory environment, and the latter because it leaves a potentially massive and highly efficient marketplace untouched and untapped.

Aside from the real threat that cyberspace users would be hit with a new privacy policy for every website they visit (and then some), switching the default rules seems to represent a step in the right direction as far as allowing the inclined user to gain the information necessary to make informed choices. Particularly, changing to a functionally necessary default rule would allow users to review privacy policies to determine the ways in which their information may be used before deciding whether to utilize a particular website or service. Such a change, although certainly imperfect, might affect an improvement over the current unregulated scenario.

C. A More Complex Approach: Propertization and Inalienabilities

Another alternative to the current regulatory failure is a particular system of propertization—that is, recognizing personal data as private property belonging to the individual—with accompanying limitations on the alienability of the property.[89] Particularly, this model incorporates restrictions preventing data collectors from transferring collected personal data to other entities without first obtaining the consent of the individual.[90] Such restrictions would give individuals some measure of control over "downstream" transactions

[89] *See* Schwartz, *supra* note 3, at 2097.
[90] *See id.* at 2098; *see also* Susan Rose-Ackerman, *Inalienability and the Theory of Property Rights*, 85 COLUM. L. REV. 931 (1985).

involving information about them.[91] If the aggregation and free transferability of personal data are to blame for the current lack of appropriate privacy protections in cyberspace, alienability restrictions could address both issues without necessarily affecting the way in which information is initially collected.[92] Professor Solove provides a poignant example of how alienability restrictions could help alleviate potential privacy problems in cyberspace in his discussion of Amazon.com's book recommendation service, which keeps track of books Amazon customers purchase and browse, analyzes these data and recommends additional books.[93] In this scenario, the problematic aspect of the transaction is not surveillance itself—the collection of the information—but the fact that Amazon.com "reserves" the right to transfer the personal information it has collected to third parties if it should sell any of its assets or go bankrupt.[94] It would have no such right under a regime in which downstream transfers of personal information were outlawed if not approved by the individual.

Alienability limitations as envisioned by Professors Solove and Schwartz would certainly be more restrictive than the default switch contemplated in Part III.A above, particularly if they were drafted to achieve maximum effectiveness. For example, Professor Schwartz envisions a regime in which the individual does not have the right to contract away his or her property rights in personal information—at least, not all at the same time.[95] The individual could not, for example, authorize Amazon.com to make downstream transfers of the information in its recommendation database during his initial transaction with Amazon. Instead, he would be given a chance to consent to such a downstream transfer only as part of a separate transaction.[96]

---

[91] *See* Schwartz, *supra* note 3, at 2098.
[92] *See* SOLOVE, *supra* note 3, at 91-92.
[93] *See id.* at 92.
[94] *See id.*
[95] *See* Schwartz, *supra* note 3, at 2098.
[96] *See id.*

This type of inalienability rule grants the consumer one power, the ability to foreclose the possibility of downstream transfers of personal information about him or herself, while taking away the individual's right to contract away all data rights in the same transaction. While laissez-faire economists and data collection industry insiders would argue that a rule of propertization and inalienability unduly burdens the consumer's right to choose, in reality the power granted to consumers under such a rule far outweighs the power usurped by it. Moreover, such a rule is likely to benefit cyberspace business over the long run. The need for additional agreements to enable downstream transfers helps to alleviate the information asymmetry that is present in the current environment, thus combating the chilling effect on e-commerce and other cyberspace activity. Although the losses occasioned by this chilling effect are not alarmingly high currently, it is very likely that these losses will increase as the current antiregulatory structure wears on and consumers become increasingly aware of the lack of privacy protections in place in cyberspace.

Implementation of a propertization and inalienability rule regarding personal information in cyberspace faces some challenges. Resistance from data collection industry groups could prove difficult to surmount, particularly since if personal information were treated as private property, the familiar arguments against restrictions on alienability of property surface.[97] On the other hand, alienability restrictions are already present with regard to other essential aspects of personhood, including one's body tissues,[98] one's children[99] and even one's self.[100] If the goal of a cyberspace privacy regime is to protect "inviolate personality" as Warren and Brandeis might

[97] Restraints on the alienability of property have never been favored under U.S. law. *See* Merrill I. Schnebly, *Restraints Upon the Alienation of Legal Interests*, 44 YALE L.J. 961, 961, 1186, 1380 (1935).
[98] *See generally* Margaret Jane Radin, *Market-Inalienability*, 100 HARV. L. REV. 1849 (1987); *see also* Brian Budds, *Toward a Just Model of Alienability of Human Tissues*, 37 U.S.F. L. REV. 757 (2003) (discussing the policy factors cited to support the inalienability rule regarding human tissues in the United States).
[99] *See* Radin, *supra* note 98.
[100] *See* U.S. CONST. amend. XII (outlawing slavery and involuntary servitude).

argue,[101] perhaps this goal is important enough to overcome the general aversion to alienability restrictions in U.S. law, as well.

Neither a default switch nor a system of propertization and inalienability would be easy to implement. However, either approach offers some protection to information privacy that does not currently exist under U.S. law. Given the problematic state of cyberspace information privacy under current law (as discussed in Parts I and II), either solution would be preferable to maintaining the status quo.

CONCLUSION

The lack of regulation of information privacy in cyberspace has created a situation in which information is available to data collectors at dangerously low prices. The potential for abuse of personally identifiable information is enormous, owing to asymmetries of information between data collectors and individuals, as well as the status of personal information as a sort of semi-commons once it is initially released. This paper has discussed the dangers of under-regulation in this arena, which include both market inefficiency and damaging effects on human dignity and self-determination, to argue that regulation is not only preferable to the current laissez-faire model, but is essential to create a balance between individual privacy rights and the business interests of data aggregators and marketers.

Regulation of information privacy in cyberspace should work to re-create transaction costs that tend to make data aggregation in the brick-and-mortar world economically unfeasible, as well as focus on data aggregation rather than specifically identified facts that are considered personal or private. This paper has discussed two possible regulatory models to further data privacy in cyberspace: a default rule reversal, and a system of propertization and inalienability.

[101] *See* Warren & Brandeis, *supra* note 33, at 195.

Propertization and limited inalienability, while admittedly restrictive and consumer-oriented, provides the best protection from the dangers presented by the current environment of inadequate data privacy protection. The additional control over information this model would allow to consumers would also facilitate equal-strength bargaining between individuals and cyberspace business interests, as well as protecting human dignity and self-determination from the increasingly dangerous encroachment of advanced and advancing technology.