A RIGHT TO PSEUDONYMITY

Ken D. Kumayama*

The advent of the Internet and the digitization of everything have resulted in greater convenience at the expense of personal privacy. Privacy advocates in the United States decry the dearth of legal protection, calling for regulation of the data collection industry along with other reforms. The industry responds with self-regulatory measures and highlights the many benefits of online services such as search engines and social networking sites. This Note echoes claims that privacy is essential to a democratic society. Requiring all users to forgo conveniences in favor of increased privacy, however, is paternalistic and undermines the very values privacy advocates seek to protect. This Note envisions technology-facilitated and legally protected "pseudonymity" as a desirable compromise, empowering users to protect their personal data as much or as little as they like.

INTRODUCTION

The Internet is more than a theoretical "place." For many, it is where we work, play, shop, learn, procrastinate, and socialize. As an ever-increasing portion of our lives migrates online, societies are coming to recognize new dimensions and manifestations of currently-held interests. One such extension is in the realm of privacy rights. Since the advent of the Internet, the collection and commodification of personal information has become cheaper, easier, and more surreptitious.[1] As the Internet moves toward an architecture further enabling the collection of such information—an architecture with increased authentication and accreditation—societies will likely react by pushing back against these invasions.[2] These invasions come not only from government,[3] but also from the personal data industry and private individuals. This results in harm both to specific individuals

---

* J.D. Candidate, University of Arizona James E. Rogers College of Law, 2009. The author would like to thank Toni Massaro, Graeme Austin, Greg Sakall, Juan Bacalski, and Matthew Bycer for their time, encouragement, and constructive criticism.

1. DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE 23–26 (2004) (describing methods used to collect personal information online).

2. *See* DIANA SACO, CYBERING DEMOCRACY: PUBLIC SPACE AND THE INTERNET 119 (2002) ("[T]echniques for ensuring electronic anonymity may be seen as direct responses to institutional digital surveillance.").

3. *See* Greg M. Schwartz, *The Panopticon Economy*, SAN ANTONIO CURRENT, Dec. 3, 2008 (describing NSA's new data mining facility in Texas), *available at* http://www.sacurrent.com/news/story.asp?id=69607.

whose personal information is abused,[4] as well as to those generally subjected to pervasive collection of personal information.[5] This Note proposes a solution to this erosion of privacy—a right to pseudonymity.[6]

The goals of this Note are twofold. First, this Note calls for individuals and policymakers to recognize a limited right to pseudonymity as an intuitive and practicable extension of privacy onto the Internet. While the exact scope of this bundle of rights—i.e., pseudonymity—cannot be determined and will likely change to keep pace with technology and culture, this Note offers some comments regarding the minimum amount of legal protection which must be afforded for such a right to be meaningful.

Second, this Note proposes a roadmap to effectuate robust protection of information privacy, which this author believes will culminate in recognition of a right to pseudonymity. Due to the global nature of the Internet, any comprehensive protection of Internet privacy must be international in scope. To that end, this Note concludes by proposing an international treaty that would address many of the current difficulties regarding harmonization and enforcement.

The subject of online privacy is enormous. Currently, both public and private actors engage in massive amounts of data collection both on- and offline. From credit card transactions and political affiliation to search engine queries and comprehensive consumer profiles, these actors compile, aggregate, analyze, and sell these data, often without the knowledge or consent of the individuals from whom the information is gathered. As a result, any comprehensive discussion of online privacy includes such issues as the roles of government, national security, free speech, and federalism. This Note only addresses the data collection practices of private actors, largely sidestepping many of these issues. Governmental interests are discussed only from the perspective of prescription and enforcement of laws, which are necessary for any meaningful protection of privacy online.

Part I explains the central role that information privacy plays in our lives and in society. As more of our lives become centered around computers and computer networks, so too do our lives become more quantifiable, indexable, and searchable. This Part seeks to impress upon readers the dangers inherent in such a system, if left unchecked.

Given the United States' preference for market self-regulation over government intervention generally, with the data collection industry as no exception, readers may question whether any government intervention is wise, let alone necessary. Part I addresses these concerns by exploring the overlap between information privacy and decisional privacy, and explores how the two merge in the

---

4. SOLOVE, *supra* note 1, at 115 ("The underlying cause of identity theft is an architecture . . . where personal information is not protected with adequate security, where identity thieves have easy access to data and the ability to use it in detrimental ways.").

5. *Id.* at 22–23.

6. A "pseudonym" is a "name that [refers] to an entity without using any of its directly identifiable characteristics, such as name, location, etc." *See* Definitions, OpenPrivacy Initiative, http://www.openprivacy.org/opd.shtml (last visited Jan. 13, 2008). "Pseudonymity," then, is the state of disguised identity resulting from the use of a pseudonym.

present context. While lawmakers in the United States have generally taken a hands-off approach to the former, the U.S. Supreme Court has evoked the protections of the U.S. Constitution on numerous occasions to safeguard the latter. This Part argues that, with the merging of information and decisional privacy, a hands-off approach to information privacy is no longer a viable option.

Part II focuses on anonymity and pseudonymity, both in "real space" and in cyberspace. The discussion begins with an overview of anonymity generally, then provides a brief overview of several characteristics of the Internet before delving into anonymity and pseudonymity in the online context. This Part concludes with a description, in general terms, of this author's conception of the nature, scope, and limitations of an online right to pseudonymity.

Part III tackles the legal difficulties inherent in any global privacy protection scheme. First, this Part describes the problems that arise when jurisdictional and choice-of-law rules are applied to activities in cyberspace. A privacy tort hypothetical illustrates and highlights these problems. This Part concludes with a set of treaty-based jurisdictional and choice-of-law rules which, this author believes, will facilitate meaningful enforcement of privacy-related and other torts that take place in the online context.

Finally, Part IV maps out the steps that domestic and international bodies must take to secure online user privacy. First, the United States must recognize that new laws and regulations governing the data collection industry are necessary, and enact laws protecting privacy on the Internet. Next, steps must be taken to educate users regarding online privacy, and technology must be developed to facilitate Internet use without sacrificing user privacy. Lastly, the international community must ratify a multilateral treaty on Internet privacy that incorporates the procedural and substantive legal rules suggested in Part III. Once these legal protections are in place, life on the Internet will flourish and an enforceable right to pseudonymity will be realized.

I. INFORMATION PRIMACY AND INFORMATION PRIVACY

Privacy is a continuously evolving concept, which scholars have long struggled to define.[7] While most agree that "individual privacy is at the core of personal identity and personal freedom,"[8] opinions vary widely regarding its exact nature and scope.[9] One common formulation, resulting from the observation that privacy is somehow intertwined with identity and autonomy, is to separate privacy broadly into two categories: "information privacy" and "decisional privacy." Information privacy is an individual's right to limit and control "the ability of others to gain, disseminate, or use information about oneself."[10] Decisional privacy

---

7. JON L. MILLS, PRIVACY: THE LOST RIGHT 21 (2008) ("As society changes, so too does its reasonable expectation of privacy . . . .").

8. *Id.* at 13.

9. *See id.* at 14 & n.40. *See generally* Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477 (2006).

10. Jed Rubenfeld, *The Right of Privacy*, 102 HARV. L. REV. 737, 740 (1989). *But see* Paul M. Schwartz, *Internet Privacy and the State*, 32 CONN. L. REV. 815, 816 (2000) (criticizing this "privacy-control" paradigm which "conceives of privacy as a personal right

involves an individual's right to make decisions regarding family, intimate relations, and other private affairs.[11] While the two certainly overlap in many situations, U.S. jurisprudence offers much greater protection for the latter than the former, only deeming decisional privacy to be a "fundamental right."[12]

This Part begins with a description of the common practices of data collection and processing. It then explores the nature and function of information privacy by comparing it to decisional privacy. This Part concludes by examining the harms that result from the collection and use of personal information, if left unchecked.

A. Data Collection and Data Mining

The collection and analysis of personal data has many important uses. For example, personal data analysis is used by private and government entities to: assess customer creditworthiness; detect fraud, abuse, and waste; improve services; promote research; manage personnel; detect criminal activities; and gather and analyze intelligence.[13]

Data mining[14] can be generally divided into two categories: descriptive and predictive tasks. People can be categorized by organizing seemingly chaotic piles of information about them into useful data sets.[15] By combing through these data sets with sophisticated, automated data mining programs, data collectors discover patterns that allow them to make educated guesses about individuals' future actions.[16] These data mining programs may reveal patterns that both users

---

to control the use of one's data"); DANIEL J. SOLOVE & MARC ROTENBERG, INFORMATION PRIVACY LAW 1 (2d ed. 2006) ("Information privacy concerns the collection, use, and disclosure of personal information.").

11. Neil M. Richards, *The Information Privacy Law Project*, 94 GEO. L.J. 1087, 1105 (2006) (book review) ("Decisional privacy involves matters such as contraception, procreation, abortion, and child rearing, and is at the center of a series of Supreme Court cases often referred to as substantive due process or the constitutional right to privacy." (quoting DANIEL J. SOLOVE ET AL., INFORMATION PRIVACY LAW 1 (2d ed. 2005))).

12. MILLS, *supra* note 7, at 122–24 (describing the scope of privacy as a fundamental right).

13. *Id.* at 14–15.

14. "Data mining" is used here to refer generally to both data matching and data mining. "Data matching" is "the computerized comparison of two or more systems of records." Daniel J. Steinbock, *Data Matching, Data Mining, and Due Process*, 40 GA. L. REV. 1, 10 (2005). "Data mining," on the other hand, is "the application of database technology and techniques—such as statistical analysis and modeling—to uncover hidden patterns and subtle relationships in data and to infer rules that allow for the prediction of future results." *Id.* at 13 (quoting U.S. GEN. ACCOUNTING OFFICE, DATA MINING: FEDERAL EFFORTS COVER A WIDE RANGE OF USES 4 (2004)).

15. *See* GREG CONTI, GOOGLING SECURITY: HOW MUCH DOES GOOGLE KNOW ABOUT YOU? 88–89 (2009).

16. Tal Z. Zarsky, *Online Privacy, Tailoring, and Persuasion*, *in* PRIVACY AND TECHNOLOGIES OF IDENTITY: A CROSS-DISCIPLINARY CONVERSATION 209, 215 (Katherine Strandburg & Daniela Stan Raicu eds., 2006).

and collectors were previously unaware of—making them powerful tools for businesses and law enforcement alike.[17]

Privacy advocates often point to the online search engine Google as the prototypical example of how the massive collection of data creates a serious threat to privacy.[18] Given the immensity of its operations, breadth of services offered, and rate of growth, there seems to be legitimate reason to worry.[19] A few examples of Google's data collection practices[20] suffice to underscore these concerns.

Google compiles a list of your searches, the web pages you view, the videos you watch, the products you purchase, and much more.[21] While the only transaction recorded in a "real space" in-store purchase is the actual sale, thanks to the digital nature of computers and the Internet, online observers are able to examine and record a consumer's every act—akin to someone looking over your shoulder as you browse the merchandise.[22] Google analyzes the data and characterizes users to create consumer profiles based on browsing behavior—labeling a user as, for example, an "Active Gamer" or a "Business Decision Maker."[23] Even without a complete set of data, data mining programs are able to predict a user's tastes and preferences—by focusing on patterns that even the keenest observer or the individual herself would overlook.[24]

Browsing the Internet while logged into Google's e-mail or other services guarantees unique identification.[25] However, once Google has acquired a critical mass of information on a particular user, Google is able to uniquely identify that individual even if he has never used Google's e-mail or other services requiring

---

17. *Cf. id. See generally* Ira S. Rubinstein et al., *Data Mining and Internet Profiling: Emerging Regulatory and Technological Approaches*, 75 U. CHI. L. REV. 261 (2008).

18. *See, e.g.*, PRIVACY INTERNATIONAL, A RACE TO THE BOTTOM: PRIVACY RANKING OF INTERNET SERVICE COMPANIES (2007), http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-553961 (explaining why Google received the lowest privacy ranking in the survey).

19. As of October 2008, Google cornered over 63% of the domestic search engine market share. Bambi Francisco, Google Increases Market Share in October, Nov. 25, 2008, http://www.vator.tv/news/show/2008-11-25-google-increases-market-share-in-october. This translates to over 4.1 billion search queries and 117 million unique users in the U.S. alone every month. CONTI, *supra* note 15, at 3; *see also id.* at 10–11 (non-comprehensive list of forty tools and services offered by Google); Miguel Helft, *Google, from Stirrer to Spoiler, Ends Microsoft's Yahoo Search*, N.Y. TIMES, May 6, 2008, at A1 (describing Google's acquisition of DoubleClick and YouTube, as well as its relationship with Yahoo!).

20. For a comprehensive overview of what types of information are collected by Google and how the information is collected, see CONTI, *supra* note 15, at 59–94 (Internet generally), 97–121 (search), 139–60 (e-mail, instant messaging, Google Groups, and mobile applications), 177–200 (maps), 205–17 (advertising), and 220–30 (embedded content).

21. *See id.* at 9–12.

22. Zarsky, *supra* note 16, at 213.

23. CONTI, *supra* note 15, at 88–89.

24. Zarsky, *supra* note 16, at 215.

25. CONTI, *supra* note 15, at 89.

one to log in.[26] Unique identification allows Google to most effectively target that individual and personalize his or her Internet experience—maximizing convenience, data collection, and use of information gleaned from analysis of personal information.[27] This cycle of collection, analysis, and use of personal data is ongoing, with new information added as it is gathered, and its analysis and use refined and reassessed accordingly.[28]

Once collected, data collectors often buy and sell personal information,[29] and Google is no exception. Google reserves the right to process personal information from third parties.[30] Google also reserves the right to sell "[a]ggregated non-personal information," which is "information [] recorded about users and collected into groups so that it no longer reflects or references an individually identifiable user"[31]—a practice called "anonymization," which is discussed below.

While Google may currently possess the largest collection of personal data in the world,[32] it is hardly alone in the market for personal information. Data collection occurs offline just as it does online, the only difference being that online data collection is more seamless and pervasive.[33] Some examples of offline information available for purchase include: "college students sorted by major, class year, and tuition payment; millionaires and their neighbors; people who have lost loved ones; . . . and tenants who have sued landlords. There are lists based on ethnicity, political opinions, and sexual orientation."[34]

In addition to the sale of sets of personal data and knowledge gained from its analysis, personal information is also "leaked" to third parties via legal compulsion, security breaches, and accidental disclosure. Internet service providers (ISPs) and online companies may be compelled to disclose personal information, including the real-world identity of users.[35] Unfortunately, data collectors have all too often inadequately protected or inadvertently disclosed data

---

26. Computer security expert and West Point professor Greg Conti argues that, given enough disclosures, Google is potentially able to uniquely identify every user. *See id.*

27. *See id.* at 80; Zarsky, *supra* note 16, at 215.

28. Zarsky, *supra* note 16, at 215.

29. MILLS, *supra* note 7, at 32.

30. Google, Google Privacy Policy, http://www.google.com/privacypolicy.html (last visited Nov. 29, 2008).

31. Google, Google Privacy Glossary, http://www.google.com/privacy_glossary.html (last visited Feb. 26, 2009).

32. Hal Roberts Watching Technology, Google Privacy Videos, http://blogs.law.harvard.edu/hroberts/2008/03/06/google-watching-personal-data-collection/ (Mar. 6, 2008, 15:21) (describing Google's store of personal data as "represent[ing] perhaps the largest, most sensitive single collection of data extant, on- or offline").

33. *See* Catherine Price, *The Anonymity Experiment*, POPSCI.COM, Feb. 8, 2008, http://www.popsci.com/scitech/article/2008-02/anonymity-experiment# (describing both real-space and cyberspace data collection practices that the author encountered while "trying to be as anonymous as possible while still living a normal life" for one week).

34. Jeff Sovern, *Opting In, Opting Out, or No Options at All: The Fight for Control of Personal Information*, 74 WASH. L. REV. 1033, 1034 (1999) (footnote omitted).

35. CONTI, *supra* note 15, at 21.

sets containing huge amounts of personal information.[36] According to one privacy watchdog, over 252 million records containing sensitive personal information have been exposed in the United States alone since January 2005.[37]

One way in which data collectors attempt to mitigate the privacy concerns inherent in these uses of personal information is through the process of "anonymization," or the removal of identifying information from data so as to safeguard anonymity while still providing useful insights.[38] For example, Google disguises the identity of the users associated with the information it harvests by only retaining IP addresses for a limited period of time.[39] While this voluntary practice, which several data collectors engage in, decreases the threats to user privacy, "anonymizing" personal information is not as meaningful as it sounds for a couple of reasons. First, data collectors who anonymize information have an interest in retaining as much of the data as possible, because stripping personal information of its unique details decreases the value of that information—a clear conflict of interest.[40] Second, removing a portion of IP addresses from search query logs—Google's current practice—is referred to as "partial anonymization."[41] While some of the identifying information is removed from the data set, there is no guarantee that the partially anonymized data cannot be recombined with other data to reveal individual identities.[42] Current research in the area of anonymization demonstrates that it is extremely difficult to determine how generalized data must become in order to avoid "de-anonymization" via combination with other data sets.[43]

At present, the U.S. federal government does not regulate the collection, use, or sale of personal information collected from online activities.[44] Compare this to the governmental regulation of the offline counterparts to the aforementioned data collection practices of companies like Google. Video rental records and cable TV subscription records are protected by state and federal

---

36. *Id.* at 18.

37. PrivacyRights Clearinghouse, A Chronology of Data Breaches, http://www.privacyrights.org/ar/ChronDataBreaches.htm (last visited Feb. 18, 2009).

38. CONTI, *supra* note 15, at 292.

39. Google currently anonymizes IP addresses after nine months and cookies after eighteen months. Google, Google Privacy FAQ, http://www.google.com/privacy_faq.html (last visited Mar. 30, 2009).

40. CONTI, *supra* note 15, at 292.

41. *See* Declan McCullagh & Elinor Mills, *How Search Engines Rate on Privacy*, CNET NEWS, Aug. 13, 2007, http://news.cnet.com/2100-1029_3-6202068.html.

42. *Id.* at 293.

43. *See* Bradley Malin, *Betrayed by My Shadow: Learning Data Identity via Trail Matching*, J. PRIVACY TECH., June 9, 2005, at 1–2, *available at* http://www.jopt.org/publications/20050609001_malin.pdf; *see, e.g.*, Bruce Schneier, *Why 'Anonymous' Data Sometimes Isn't*, WIRED.COM, Dec. 13, 2007, http://www.wired.com/politics/security/commentary/securitymatters/2007/12/securitymatters_1213 (describing researchers' successful "de-anonymization" of some data taken from anonymized movie rankings by Netflix customers, via combination with other publicly available information).

44. *See* SOLOVE, *supra* note 1, at 67–72 (listing privacy-protecting laws in the United States).

legislation.[45] Additionally, nearly all states have enacted legislation protecting the identity of library patrons.[46] These laws are based upon the underlying recognition of an individual's "right to read or observe what he pleases—the right to satisfy his intellectual and emotional needs in the privacy of his own home."[47]

The dearth of regulation of the online (and, as we will see, offline) data collection industry in the United States is a consequence of deliberate policy decisions. The patchwork nature of the regulations that comprise the U.S. regulatory framework and the policy decisions behind them come into focus when contrasted with the comprehensive regulations adopted by the European Union. Perhaps the primary source of this difference is U.S. policymakers' steadfast faith in the ability of markets generally to self-regulate.[48] While the European Union has enacted broad proactive measures to safeguard personal information, the United States has consistently opted to enact laws protecting only discrete categories of personal information in reaction to actual instances where affirmative steps were deemed necessary to protect people's privacy.[49] Furthermore, narrowly drafted data protection laws allow lawmakers to minimize conflict with countervailing values such as free speech and national security, as well as with the data collection industry.[50] Where the U.S. legal system values free speech over protection of personal information, the European Union has chosen to strike a different balance, favoring greater protection of information privacy.[51] The following section will discuss the nature of privacy generally and compare in greater detail the conceptions of privacy in the United States and European Union.

---

45. Julie E. Cohen, *A Right to Read Anonymously: A Closer Look at "Copyright Management" in Cyberspace*, 28 CONN. L. REV. 981, 1031 & n.211 (1996) (videotape rentals); *id.* at 1031 & n.212 (cable TV records).

46. *Id.* at 1031 & n.213.

47. Stanley v. Georgia, 394 U.S. 557, 565 (1969) (striking down state law criminalizing private possession of "obscene"materials). *See* Neil M. Richards, *Intellectual Privacy*, 87 TEX. L. REV. 387, 389 (2009) (discussing the importance of "the ability . . . to develop ideas and beliefs away from the unwanted gaze or interference of others" to the rights guaranteed by the First Amendment and, ultimately, to democracy).

48. Joel R. Reidenberg, *Privacy in the Information Economy: A Fortress or Frontier for Individual Rights*, 44 FED. COMM. L.J. 195, 209 (1992) (describing domestic government's approach to privacy laws as "deriv[ing] from the traditional American fear of government intervention in private activities and the reluctance to broadly regulate industry").

49. *See, e.g.*, *supra* notes 45–46 and accompanying text. For a comprehensive overview of the patchwork of privacy-protecting statutes in the United States, *see* SOLOVE, *supra* note 1, at 69 (explaining that the Video Privacy Protection Act, which "prohibits videotape service providers from disclosing the titles of the videos a person rents or buys," was enacted "[a]fter reporters obtained Supreme Court nominee Robert Bork's videocassette rental data"); MILLS, *supra* note 7, at 130–70.

50. MILLS, *supra* note 7, at 130–31.

51. James Q. Whitman, *The Two Western Cultures of Privacy: Dignity Versus Liberty*, 113 YALE L.J. 1151, 1208 (2004) ("[T]he American resistance to Warren and Brandeis has always been a resistance founded on two values in particular: the value of the free press, and the value of the free market."); *see also* MILLS, *supra* note 7, at 228 ("A major reason for the failures of privacy remedies are our First Amendment protections.").

B. Information Privacy and Decisional Privacy

In the United States, Samuel Warren and Louis Brandeis first conceived of the right to privacy in 1890 as "the right to be let alone."[52] In setting out their vision of the right to privacy, Warren and Brandeis sought to provide a legal basis for preventing intrusive reporters from publishing photographs and information pertaining to the activities that take place within the confines of one's own home.[53] Seventy years later, Dean William Prosser sought to quantify the various privacy interests at stake by analyzing the case law that emerged from Warren and Brandeis' seminal work.[54] He categorized harms to privacy as falling into one of four types: (1) intrusion upon a plaintiff's seclusion or solitude, or into her private affairs; (2) public disclosure of embarrassing private facts about the plaintiff; (3) publicity that places the plaintiff in a false light in the public eye; and (4) appropriation, for the defendant's advantage, of the plaintiff's name or likeness.[55]

The Supreme Court first recognized the constitutional protections of privacy in *Griswold v. Connecticut*, envisioning the right to privacy as emanating from the "penumbras" of the Bill of Rights.[56] The *Griswold* Court struck down a state law that forbade the use of contraceptives, holding that the law impermissibly intruded upon "the right of marital privacy."[57] More recently, the Court in *Lawrence v. Texas* discarded the penumbral theory, looking instead to the substantive due process rights guaranteed by the Fourteenth Amendment for the constitutional basis of the right to privacy.[58] The Court struck down a Texas statute outlawing homosexual relations, finding the Texas statute's "intrusion into the personal and private life of the individual" to be an unjustified violation of privacy.[59]

Often juxtaposed with this sphere of personal autonomy free from government interference is "information privacy."[60] Although the idea of information privacy has been around in the United States for some time,[61] most U.S. case law relating to the right to privacy deals with decisional privacy.[62]

---

52. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 195 (1891) (quoting THOMAS M. COOLEY, A TREATISE ON THE LAW OF TORTS 29 (2d ed. 1888)).

53. *Id.* at 206.

54. William L. Prosser, *Privacy*, 48 CAL. L. REV. 383, 384–410 (1960).

55. *Id.* at 389.

56. Griswold v. Connecticut, 381 U.S. 479, 484 (1965) (deriving the constitutional basis for the right to privacy as "eminat[ing]" from the "penumbras" of the First, Third, Fourth, Fifth, and Ninth Amendments).

57. *Id.* at 486 (Goldberg, J., concurring).

58. *See* Lawrence v. Texas, 539 U.S. 558, 578 (2003).

59. *Id.*

60. *See* sources cited *supra* note 10.

61. *See* Whalen v. Roe, 429 U.S. 589, 598–600 (1977) (acknowledging that the Court's privacy jurisprudence "involve[s] at least two different kinds of interests"—"the individual interest in avoiding disclosure of personal matters" and "the interest in independence in making certain kinds of important decisions").

62. *See* Roe v. Wade, 410 U.S. 113, 152–53 (1973) (noting that "the right of personal privacy" includes "only personal rights that can be deemed 'fundamental,'" such as

Information privacy has generally received governmental protections only in limited scenarios, in response to specific abuses of personal information.[63]

In Europe, the concept of privacy has evolved quite differently from the United States.[64] Placing less emphasis on privacy-as-liberty, the Europeans view privacy as essential to personal dignity.[65] Although this dignity-centric paradigm is by no means absolute, its influence is felt throughout the European legal systems.[66] For example, the Federal Constitutional Court of (then) West Germany held in 1983 that an individual's "informational self-determination" was an essential personal right protected by the German Constitution.[67] This recognition has been adopted and expressed in the European Union's Charter of Fundamental Rights, which contains language expressly recognizing the right of individuals to protect their personal information.[68] This paradigmatic difference helps account for the formation of the largely self-regulating personal information market in the United States, as contrasted with the much more active regulatory role that the EU government has taken.[69]

When juxtaposed, the American and European conceptions of privacy—the former championing freedom and liberty, the latter defending honor and dignity—seem quite different. Yet at a fundamental level, information and decisional privacy both secure individuals' right to self-identity.[70] This allows for the self-development and, ultimately, the self-actualization of individuals, thus benefiting both society and its members.[71] To further explore the intersection

---

"procreation, contraception, family relationships, . . . child rearing and education" (citations omitted)).

63. *See* sources cited *supra* note 49.

64. *See generally* Whitman, *supra* note 51.

65. *Id.* at 1160–64.

66. *See, e.g.*, Brian T. McCartney, *"Creepings" and "Glimmers" of the Moral Rights of Artists in American Copyright Law*, 6 UCLA ENT. L. REV. 35, 71–72 (1998) (describing EU copyright laws as having strong protections for authors' moral rights while "America is still a long way from recognizing the moral right").

67. Bundesverfassungsgericht [BVerfG] [Federal Constitutional Court] Dec. 15, 1983, 65 Entscheidungen des Bundesverfassungsgerichts [BVerfGE] 1 (F.R.G.), *available at* http://www.servat.unibe.ch/dfr/bv065001.html.

68. Charter of Fundamental Rights of the European Union, arts. 7–8, 2000 O.J. (C 364) 1, 10.

69. Joel R. Reidenberg, *Resolving Conflicting International Data Privacy Rules in Cyberspace*, 52 STAN. L. REV. 1315, 1330–31 (2000) (comparing "comprehensive data protection law" predominantly found outside United States with treatment of data privacy as "market issue rather than a basic political question" in United States).

70. JUDITH WAGNER DECEW, IN PURSUIT OF PRIVACY 63 (1997) (asserting that all forms of privacy are at root concerned with "the right to shape the 'self' that one presents to the world, and on the basis of which the world in turn shapes one's existence"); *see id.* at 113 (noting that dominant theme in constitutional privacy is "whether a decision or action is fundamental to one's self-identity"). Recognition of the close relationship between action and identity goes back at least to Dogen Zenji's philosophy in the thirteenth century. DOGEN ZENJI, *The Time-Being*, *in* MOON IN A DEWDROP: WRITINGS OF ZEN MASTER DOGEN 76–83 (Kazuaki Tanahashi ed., Robert Aitken et al. trans., 1985).

71. ANTHONY GIDDENS & CHRISTOPHER PIERSON, CONVERSATIONS WITH ANTHONY GIDDENS 23 (1998) (describing self-actualization as "realizing one's own identity

between these two components of the right to privacy, this author borrows from the works of sociologist Anthony Giddens, who has written extensively on the nature of identity in modern societies.

In exploring the importance of "identity" to individuals and society, Giddens noted that identity requires self-awareness.[72] Rejecting the idea that identity does not exist but merely seems to manifest through individuals' relationships in society, he instead posited that identity was something "routinely created and sustained in the reflexive activities of the individual."[73] Identity was not to be located in one's actions nor one's interactions with others.[74] Instead, identity is "*the self as reflexively understood by the person in terms of her or his biography*."[75] Identity, then, is a self-authored "ongoing 'story' about the self"—a narrative about "how we have become and [] where we are going."[76]

While decisional privacy clearly protects an individual's most intimate decisions from government intrusion, implicit in the protection of this most private area of one's life is the recognition that these are the types of decisions many individuals consider central to their personal narrative, and thus to their identity.[77] Information privacy, on the other hand, does not play as direct a role in the creation of the self—much as a third party's knowledge or opinion of someone may influence, but generally does not redefine, how she conceives of herself.[78] That is, if autonomy and identity are neighbors, then dignity lives up the street.

---

through personal and social encounters[, which is] . . . a basic condition of modern social life"); Antoinette Rouvroy & Yves Poullet, *The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy*, *in* REINVENTING DATA PROTECTION 8 (Serge Gutwirth et al. eds., forthcoming 2009), *available at* http://works.bepress.com/cgi/viewcontent.cgi?article=1006&context=antoinette_rouvroy (describing "informational self-determination" as "an individual's control over the data and information produced about him[, which] is a . . . pre-condition for him to live an existence that may be said 'self determined'").

72. ANTHONY GIDDENS, MODERNITY AND SELF-IDENTITY: SELF AND SOCIETY IN THE LATE MODERN AGE 52 (1991) ("The 'identity' of the self . . . presumes reflexive awareness."); *see also* MILLS, *supra* note 7, at 20–21 & n.64 (noting the importance of self-awareness).

73. GIDDENS, *supra* note 72, at 52.

74. *Id.* at 54 ("A person's identity is not to be found in behaviour, nor—important though this is—in the reactions of others . . . .").

75. *Id.* at 53.

76. *Id.* at 54 (quoting CHARLES TAYLOR, SOURCES OF THE SELF: THE MAKING OF THE MODERN IDENTITY 47 (1992)). What one is doing is of primary importance to the autobiography, as are the reasons for the doing—yet Giddens focuses less on the doing and more on the "'going on' in the variegated settings of our lives." *Id.* at 35.

77. *See* Roe v. Wade, 410 U.S. 113, 152–53 (1973) (noting that "the right of personal privacy" includes "only personal rights that can be deemed 'fundamental,'" such as "procreation, contraception, family relationships, . . . child rearing and education" (internal citations omitted)).

78. *But see* Ann Branaman, *Introduction* to ERVING GOFFMAN, THE GOFFMAN READER xlv, xlviii (Charles Lemert & Ann Branaman eds., 1997) (summarizing Goffman's conception of the self as "the mask the individual wears in social situations, but it is also the human being behind the mask who decides which mask to wear").

Information privacy is a necessary precondition for the formation of one's identity.[79] That being said, its primary function is not the creation of identity but its maintenance.[80] Information privacy allows for greater freedom of action and interaction by protecting individuals from "being misdefined and judged out of context in a world . . . in which information can easily be confused with knowledge."[81] Only by protecting the creation and maintenance of identity—which derives from an individual's actions and interactions—can individuals self-actualize and participate fully in a democratic society.[82]

In summary, while the information-decisional dichotomy can be useful, dogmatic adherence to the distinction can undermine the core values that "decisional privacy" is intended to protect.

C. Why Protect Information Privacy?

Thus far in the United States, the line drawn between the fundamental right of decisional privacy and the lesser right of information privacy has been in keeping with our society's balance of many competing values.[83] This section explores how technological progress has shifted the calculus, such that information privacy should be granted increased protection in certain circumstances.[84] The ubiquity of the Internet and our entrance into a new, digital age allows for unprecedented collection of personal information on a mind-boggling scale.[85] How these changes affect society is cause for great concern.

The privacy concerns surrounding the collection and use of personal information largely depend upon whether that information can be traced back to the individual from whom it came. Many privacy concerns may be alleviated if

---

79. Rouvroy & Poullet, *supra* note 71, at 18 ("[T]otal transparency would impair the possibility for individuals to freely develop their personality. They need some 'secrecy, anonymity and solitude,' 'withdrawal and concealment' in order to reflect on their own preferences and attitudes, or, in other words, to reflexively make and revise choices in life, as well as to develop meaningful relationships with others." (citation omitted)).

80. *See* Helen Nissenbaum, *Protecting Privacy in an Information Age: The Problem of Privacy in Public*, 17 LAW & PHIL. 559, 583 (1998) ("In having the power to share information discriminately, people are able to define the nature and degree of intimacy of various relationships . . ., an important aspect of personal autonomy.").

81. JEFFREY ROSEN, THE UNWANTED GAZE: THE DESTRUCTION OF PRIVACY IN AMERICA 8 (2000).

82. *See* sources cited *supra* note 70; MILLS, *supra* note 7, at 26 ("Privacy is an integral part of the amalgamation of values that define a healthy society.").

83. *See* MILLS, *supra* note 7, at 124–30 (discussing court cases involving information privacy).

84. *See* Elbert Lin, *Prioritizing Privacy: A Constitutional Response to the Internet*, 17 BERKELEY TECH. L.J. 1085, 1118–44 (2002) (advocating for constitutional protections of information privacy at the state level).

85. *See* CONTI, *supra* note 15, at 3 (describing the amount of digital information produced and in existence on the Internet); Zarsky, *supra* note 16, at 212–13; *see also* John Markoff, *You're Leaving a Digital Trail. What About Privacy?*, N.Y. TIMES, Nov. 30, 2008, *available at* http://www.nytimes.com/2008/11/30/business/30privacy.html?scp=3&sq=markoff%20privacy&st=cse (describing use of digital technology to collect real-space personal information and conduct "reality-mining").

data are either collected so as to preserve anonymity or anonymized after collection. Recall, however, that no U.S. laws currently require data collectors to take such privacy-friendly steps, and current research shows that anonymizing data is easier said than done.[86] The resulting harms, described below, illuminate the need for greater protection of information privacy.

1. Self-Censorship and Chilling Free Expression

If every word someone types can be traced back to that person, people will likely choose their words with greater care. While more thoughtful communication may not be a bad thing, knowledge of ongoing surveillance will inevitably result in self-censorship.[87] The fact that an individual's words, once uttered, may be chiseled onto the Internet's memory—perhaps for all time—will likely give some individuals added pause.[88] This propensity to self-censor further increases in countries where free speech is more thinly protected, such as India and China.[89]

The danger of self-censorship applies equally to expressive activities as it does to expression through words. For example, knowledge of an individual's affiliations or "social network" could harm her right of expressive association, especially when that individual is a minority (e.g., McCarthyism and racism).[90]

2. Hindering Free Thought

The right to access information without being monitored has profound First Amendment implications. Most fundamentally, the American "tradition of anonymous exploration and inquiry" is a prerequisite to freedom of thought.[91] Knowledge that one is being monitored may have a chilling effect on access to that information.[92] Considering the wealth of information on the Internet and the

---

86. *See supra* notes 38–43 and accompanying text.

87. Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193, 1260 (1998) ("surveillance leads to self-censorship").

88. Bruce Schneier, *The Tech Lab: Bruce Schneier*, BBC NEWS, Feb. 26, 2009, http://news.bbc.co.uk/1/hi/technology/7897892.stm ("Welcome to the future, where everything about you is saved."); J.D. Lasica, *Digital Footsteps*, SALON, Nov. 1998, http://www.jdlasica.com/ articles/digital.html ("Today, our pasts have become etched like a tattoo [sic] into our digital skins."); *see also* SOLOVE, *supra* note 1, at 26.

89. Michael Arrington, *Hit Pause on the Evil Button: Google Assists in Arrest of Indian Man*, TECHCRUNCH.COM, May 18, 2008, http://www.techcrunch.com/2008/05/18/hit-pause-on-the-evil-button-google-assists-in-arrest-of-indian-man/ (Google provided information to Indian authorities about individual who posted "vulgar language about Sonia Gandhi," resulting in his identification and punishment.); *Yahoo "Helped Jail China Writer,"* BBC NEWS, Sept. 7, 2005, http://news.bbc.co.uk/2/hi/asia-pacific/4221538.stm.

90. *See* NAACP v. Alabama, 357 U.S. 449, 462 (1958) (prohibiting Alabama from forcing NAACP to disclose identities of its members, as such action would violate members' right to expressive association).

91. *See* Cohen, *supra* note 45, at 1010–13; Richards, *supra* note 47 at pt. II (offering a "broad [normative] theory of why and how we should protect privacy in intellectual explorations").

92. Cohen, *supra* note 45, at 1008.

potential for pervasive surveillance, the chill on individuals' intellectual inquiry may be substantial.

Free thought may also potentially be actively hindered by those who control access to information. With enough power, one could conceivably censor, control, or alter content on the Internet. An entity such as Google, which can monitor users' activities and alter the content served accordingly, may also act as a gatekeeper and censor.[93] For example, China uses Google's technology to censor information it deems dangerous.[94] As societies come to rely ever increasingly on the Internet for information, those who control our access to information may also be able to influence the popularity of ideas—a frightening thought for any democracy.

3. Abuse of Personal Data

Personal information can be intentionally or negligently abused to cause emotional, financial, or further instances of privacy-related harms.[95] While this has always been the case, the current state of pervasive data collection combined with the lack of incentives to properly secure this wealth of information has exacerbated the potential for misuse.[96] Recall also that sensitive data are often sold or leaked to third parties.[97] In one extreme case, a data broker sold a woman's work address to a stalker, resulting in the woman's death.[98]

4. Data Collection and Autonomy

George Orwell's book *1984* is an oft used example of how pervasive surveillance can undermine one's autonomy.[99] In this grim view of one possible future, the government—known as "Big Brother"—tirelessly observes its citizens, controlling all aspects of their lives to the point of controlling their very thoughts.[100] The extreme oppression conceived in Orwell's fictional world is largely due to human, rather than technological, observation of citizens' private lives, a crucial distinction between that world and ours.[101] Although computer

---

93. *See* Jeffrey Rosen, *Google's Gatekeepers*, N.Y. TIMES, Nov. 30, 2008, at MM50, *available at* http://www.nytimes.com/2008/11/30/magazine/30google-t.html?_r=2&pagewanted=1&ref=magazine.

94. Elinor Mills, *Google to Censor China Web Searches*, CNET NEWS, Jan. 24, 2006, http://news.cnet.com/Google-to-censor-China-Web-searches/2100-1028_3-6030784.html.

95. MILLS, *supra* note 7, at 33.

96. While some states have enacted additional privacy protections, such as the California security-breach notification statute, there are currently no other penalties nor liabilities for such incidents. *See* MILLS, *supra* note 7, at 167–68 (citing CAL. CIV. CODE § 1798.29 (2003); §§ 1798.82–.84 (2005)).

97. *See supra* notes 29–37 and accompanying text.

98. SOLOVE, *supra* note 1, at 54 (discussing *Remsburg v. Docusearch, Inc.*, 816 A.2d 1001 (N.H. 2003)).

99. *See, e.g.*, *id.* at 29–35 (citing GEORGE ORWELL, 1984 (1949)).

100. *Id.* at 29.

101. Daniel J. Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy*, 53 STAN. L. REV. 1393, 1417–18 (2001).

monitoring is much less invasive, it arguably poses significant threats to privacy for two reasons. First, much of the data being collected may be uniquely identifiable and traceable to the individual described by that data.[102] Second, as artificial intelligence becomes increasingly sophisticated, so too does the invasiveness of computerized surveillance.[103]

Additionally, the present use of our personal information threatens to undermine how we react in more subtle ways. For example, data collection and analysis could result in an effective tool for manipulation by pushing a user's emotional buttons. Professor Tal Zarsky explains:

> [S]hame, guilt, and panic are emotions that are effectively invoked by today's advertisers to persuade consumers to take particular actions. Specific knowledge as to the preferences and personality traits of every specific user can inform advertisers as to which specific *emotional* responses they must try to invoke [] to move a consumer to act. Knowledge as to what stimuli will likely induce a desired response may now be available to today's content providers as a result of constantly tracking consumers' ongoing conduct.[104]

The worry is that, as information about each consumer increases along with the efficacy of the technologies, marketers will develop increasingly powerful tools of persuasion, such as "specially tailored marketing pitches and advertisements that will capitalize on [individuals'] vulnerabilities and take advantage of their weaknesses," such that the consumer is convinced to take an action that, if given the opportunity to think things over in solitude, she would not have taken.[105] While this form of manipulation is primarily employed by commercial marketers, political engines have also begun exploring possible ways to use data mining to their advantage.[106] While the empirical evidence regarding the efficacy of these tools of persuasion remains inconclusive, many scholars and privacy advocates fear that the threat is genuine.[107]

5. Data Collection and Identity

Although the primary function of information privacy is not the creation of an individual's identity, it is a necessary ingredient for the maintenance of identity and the attainment of self-actualization.[108] Formation of identity as a reflexive exercise requires that individuals have solitude, a chance to withdraw and "reflect on their own preferences and attitudes, . . . as well as to develop

---

102. *See supra* notes 25–26 and accompanying text.

103. *Cf.* CONTI, *supra* note 15, at 141 (noting that "Google is able to [detect] . . . 'catastrophic events or tragedies'").

104. Zarsky, *supra* note 16, at 218.

105. *Id.* at 219.

106. *See* Thomas B. Edsall, *Democrats' Data Mining Stirs an Intraparty Battle*, WASH. POST, Mar. 8, 2006, at A01, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2006/03/07/AR2006030701860_pf.html.

107. Zarsky, *supra* note 16, at 219. On a related note, it may also be possible for analysis of personal data to turn up names of those who are more easily fooled by deceptive campaigns. *Id.* at 219 n.18.

108. Rouvroy & Poullet, *supra* note 71, at 18.

meaningful relationships with others."[109] If too much erosion of information privacy is permitted, the result would be equivalent to a loss of decisional privacy: a society lacking in free thought, free expression, and free will. This undesirable result is most correctly characterized not as a separate harm resulting from pervasive data collection, but as the culmination of the many harms described above.

In addition to impeding individuals' creation of their own identities, the systematic labeling and categorizing of individuals may result in increased similarity of interests among individuals who are similarly grouped.[110] While this result may be a marketer's dream, it seems hardly desirable in a pluralistic democracy such as the United States. As databases are populated with greater amounts of personal data, perhaps allowing for a more nuanced analysis of our personalities, the dangers of stereotyping may decrease, but at the expense of our privacy. While the above examples indicate the harms resulting from the current state of the Internet and the data industry, these intrusions are only likely to increase as the technology improves and our reliance on the Internet increases.

Ultimately, how much value one ascribes to her privacy is a matter for each individual to decide. Some people prefer the convenience of receiving targeted advertisements and are unfazed by the prospect of having their e-mails and web browsing habits collected. Others would gladly give up some convenience for increased privacy protection. Part II explains how pseudonymity gives users the tools they need to decide what balance of privacy and convenience best meets their needs.

II. ANONYMITY AND PSEUDONYMITY

Anonymity and pseudonymity describe limitations on information that an actor discloses when participating in a particular transaction.[111] The two concepts are often conflated, particularly in the context of the Internet. Before delving into the roles that anonymity and pseudonymity play in the Internet context, brief descriptions of the two concepts are provided.

A. General Contours of Anonymity and Pseudonymity

By withholding all information extrinsic to a transaction, anonymity provides protection for an actor in two ways. First, it shields the actor from the prejudices and biases of others while also permitting the actor to hide her own bias or self-interest.[112] Second, anonymity protects the actor from any negative

---

109. *Id.* (footnote omitted).

110. *See* Solove, *supra* note 101, at 1425 ("Rather than provide a nuanced portrait of our personalities, [databases] capture the stereotypes and the brute facts of what we do without the reasons.").

111. Tal Z. Zarsky, *Thinking Outside the Box: Considering Transparency, Anonymity, and Pseudonymity as Overall Solutions to the Problems of Information Privacy in the Internet Society*, 58 U. MIAMI L. REV. 991, 1024 (2004) (describing anonymity as bringing the flow of personal information "to an immediate halt").

112. A. Michael Froomkin, *Flood Control on the Information Ocean: Living with Anonymity, Digital Cash, and Distributed Databases*, 15 J.L. & COM. 395, 403, 409 (1996)

repercussions flowing from the transaction, shielding the actor both from accountability for her unlawful acts and from any unwarranted reprisals.[113] Due to these protections, anonymity offers peace of mind, while a lack thereof can have a chilling effect upon speech and activities.[114]

Anonymity in the United States has a long history. *The Federalist Papers*, authored jointly by James Madison, Alexander Hamilton, and John Jay, and published between 1787 and 1788, were written under the pseudonym "Publius."[115] The Supreme Court has recognized anonymous political speech as an essential building block of a free, democratic society, declaring it "an honorable tradition of advocacy and dissent" protected by the First Amendment.[116] The Court also recognized anonymity as essential to the constitutionally protected right to freedom of association, noting that "[i]nviolability of privacy in group association may . . . be indispensable to preservation of freedom of association, particularly where a group espouses dissident beliefs."[117] In the same vein, for those who fight against government oppression, both domestically and abroad, the cloak of anonymity permits free speech where otherwise there would be none.[118]

("[A]nonym[ity] . . . makes it more difficult to identify the self interest or bias underlying an argument. . . . [T]he writer must be judged solely on their content as there is literally nothing else to go by." (internal quotation marks omitted)); *see, e.g.*, Andrew Martin, *Whole Foods Executive Used Alias*, N.Y. TIMES, July 12, 2007, at C1 (describing Whole Foods CEO's pseudonymous online disparaging comments regarding Wild Oats, presumably to lower acquisition cost).

113. *See* McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 343 (1995) ("[T]he secret ballot [permits the exercise of] the hard-won right to vote one's conscience without fear of retaliation."); *id.* at 385 (Scalia, J., dissenting) ("[Anonymity] facilitates wrong by eliminating accountability . . . .").

114. ALAN F. WESTIN, PRIVACY AND FREEDOM 31 (1967) ("Knowledge or fear that one is under systematic observation in public places destroys the sense of relaxation and freedom that men seek in open spaces and public arenas."); *see also* U.S. v. White, 401 U.S. 745, 787–88 (1971) (Harlan, J., dissenting).

115. *McIntyre*, 514 U.S. at 343 n.6.

116. *Id.* at 357 (dealing specifically with anonymous political pamphleteering); *see also* Buckley v. Am. Constitutional Law Found., Inc., 525 U.S. 182, 200 (1999) (holding, *inter alia*, state statute requiring petitioners to wear identification badges bearing petition circulator's name violated First Amendment); Watchtower Bible & Tract Soc'y, Inc. v. Vill. of Stratton, 536 U.S. 150, 169 (2002) (finding that ordinance requiring solicitors to obtain permit prior to engaging in door-to-door activities and to display the permit upon demand unconstitutionally abridged solicitors' right to free *religious* speech).

117. NAACP v. Alabama, 357 U.S. 449, 462 (1958) (prohibiting Alabama from forcing NAACP to disclose identities of its members, as such action would violate members' right to expressive association).

118. *McIntyre*, 514 U.S. at 357 (citing JOHN STEWART MILL, ON LIBERTY AND CONSIDERATIONS ON REPRESENTATIVE GOVERNMENT 3–4 (Ronald Buchanan McCallum ed., 1947)) ("Anonymity is a shield from the tyranny of the majority."); *see, e.g.*, *id.* at 360–67 (Thomas, J., concurring) (describing "practices and beliefs held by the Founders concerning anonymous political articles and pamphlets").

Pseudonymity gives a name to an otherwise nameless, faceless actor. With a name comes the ability to accrue reputational capital.[119] This permits the actor to receive the same protections afforded by anonymity, but with the additional benefits that come with reputation—most notably, the ability to form enduring relationships.[120] The actor is still permitted to hide her self-interest if she so chooses, and she remains protected from the prejudices of others, excepting any prejudices toward the reputation of the pseudonymous persona.[121] Additionally, the actor remains unaccountable for her actions, thus being equally protected from oppression.[122]

The reputational dimension of pseudonymity allows the actor to reap the benefits of the goodwill sown by previous actions.[123] As the reputation gains more value, the actor will have greater incentive to avoid taking actions harmful to the persona's good name.[124] Therefore, a pseudonymous persona that fails to abide by the norms that govern a relationship does so at risk to the reputational capital it has accrued.[125] Due to this characteristic limitation of the repercussions of an act to the pseudonymous persona, Professor David G. Post has likened pseudonymity to the limited liability enjoyed by corporate entities.[126] Despite the differences between anonymity and pseudonymity, the law in the United States has not differentiated between the two, as both retain the characteristic shield against oppression that the Supreme Court has deemed worthy of constitutional protection in limited situations.[127]

B. Characteristics of the Internet

Before discussing the nature of anonymity and pseudonymity in cyberspace, it is necessary to first review four key characteristics that distinguish cyberspace from real-space. First, the Internet is borderless—it transmits information without regard to geographical boundaries.[128] As a result, information

---

119. David G. Post, *Pooling Intellectual Capital: Thoughts on Anonymity, Pseudonymity, and Limited Liability in Cyberspace*, 1996 U. CHI. LEGAL F. 139, 160 (1996) ("[B]y serving as storehouses of reputational capital, pseudonymous entities add value to social interaction in a way that anonymous speech does not.").

120. *Id.*

121. *See id.*

122. *Id.* at 166 (pseudonymity protects both reputation and assets of actor); *see id.* at 160 (noting that pseudonymity enjoys the same lack of accountability as anonymity).

123. *See id. Cf.* LAWRENCE LESSIG, CODE VERSION 2.0 88–111 (2006) (describing various online communities, most of which facilitate pseudonymous interactions).

124. LESSIG, *supra* note 123, at 102 ("Where community is thick, norms can regulate.").

125. *See* Post, *supra* note 119, at 166.

126. *See id.* at 160–61.

127. *See, e.g.*, McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 341 (1995) (conflating anonymous speech with "authors writing under assumed names").

128. *See* ACLU v. Reno, 521 U.S. 844, 851 (1997) ("Taken together, these tools constitute a unique medium— known to its users as 'cyberspace'—located in no particular geographical location but available to anyone, anywhere in the world, with access to the Internet."). However, China is attempting, with some success, to regulate the information that passes within its borders. *See generally* REPORTERS WITHOUT BORDERS, CHINA:

and online activities that are perfectly legal in one jurisdiction may be banned in other jurisdictions, leading to complex jurisdictional and choice-of-law issues.[129]

Second, the Internet has the potential to become the most *regulable* space ever created.[130] Although the Internet remains largely unregulated, the technology upon which the Internet and its constituent computers rely can be modified, for example, to record every keystroke and mouse-click you make, every webpage you read, and every search you enter.[131] As mentioned in Part I, this is already happening to some degree, though it has yet to reach its maximum potential.[132]

Third is the Internet's potential for user anonymity. While the average user is no longer able to access the Internet's wealth of information anonymously,[133] anonymous Internet usage is still possible for the most sophisticated users.[134] Much like the degree of regulation on the Internet, the amount of anonymity or pseudonymity afforded to Internet users is ultimately a question of architecture and, thus, a matter of policy.[135]

Fourth, and finally, is the concept of traceability.[136] Traceability is the ability of someone, most often a government, to trace an action back to its source.[137] The concept of traceability applies to both anonymous and pseudonymous activities.[138] Thus, while traceable pseudonymity would permit the government to hold a user accountable, an untraceable pseudonymous user

---

JOURNEY TO THE HEART OF INTERNET CENSORSHIP (2007), http://www.rsf.org/IMG/pdf/Voyage_au_coeur_de_la_censure_GB.pdf.

129. For example, online gambling is currently illegal in the United States. 31 U.S.C. § 5363 (2006). *But see* JACK GOLDSMITH & TIM WU, WHO CONTROLS THE INTERNET? ILLUSIONS OF A BORDERLESS WORLD 49–125 (2006) (describing how the Internet is becoming more bordered).

130. LESSIG, *supra* note 123, at 38 ("[I]f it were so designed, then the Net could become . . . the most regulable space that man has ever known.").

131. *See* Peter Whoriskey, *Every Click You Make*, WASH. POST, Apr. 4, 2008, at D01, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2008/04/03/AR2008040304052.html.

132. *See, e.g.*, sources cited *supra* note 20.

133. *But see* LESSIG, *supra* note 123, at 43–45.

134. *See id.* at 224 ("If implemented properly, there is absolutely no technical way to trace [a] message [sent using privacy enhancing tools].").

135. John Markoff, *A New Internet?*, N.Y. TIMES, Feb. 15, 2009, at WK1 ("A more secure network is one that would almost certainly offer less anonymity and privacy."); *see* GOLDSMITH & WU, *supra* note 129, at 156–57 (explaining that the "First Amendment['s] . . . values . . . are certainly not written into the Internet's architecture").

136. In the field of identity management, this is often referred to as "linkability."

137. *See* Post, *supra* note 119, at 150 (defining traceability as "the ease with which additional information . . . about the identity of the sender can be obtained"); Zarsky, *supra* note 111, at 1031 (describing untraceable pseudonymity as the use of aliases "which cannot be traced back to his or her physical persona by anyone or in any way").

138. *See* Froomkin, *supra* note 112, at 417–24 (describing traceable and untraceable pseudonymity and anonymity).

remains untouchable. Presumably, either type of pseudonymity could be incorporated into the architecture of the Internet.[139]

C. Anonymity and Pseudonymity on the Internet

On the Internet, the only difference between an anonymous and pseudonymous persona is whether the user chooses to use the persona more than once.[140] The more often a persona is used and the more relationships it creates, the more reputational capital it can accrue.[141] The lack of context surrounding communications over the Internet allows users to easily adopt pseudonymous personas, thus amplifying the attributes of anonymity and pseudonymity described above.[142] For instance, an anonymous pamphleteer must take great care to avoid revealing his identity, while an anonymous e-mail can be sent with the push of a button.

Untraceable online pseudonymity provides two types of benefits to users. First, it protects privacy by mitigating many of the negative effects of personal data collection. As described in Part I, the data collection industry presents several threats to the individual: (1) self-censorship of expression; (2) hindrance of free thought; (3) misuse of personal information; (4) interference with autonomy; and (5) interference with identity.[143] An Internet architecture permitting untraceable pseudonymity mitigates or eliminates all of these threats. Self-censorship of expression and intellectual inquiry does not occur if online activities are untraceable.[144] Personal information collected from a pseudonymous persona can be misused to harm the persona but never the persona's real-space counterpart.[145] Also, the possibility of information being made unavailable to select individuals is decreased, as anyone targeted can simply create a new persona to access the information.

---

139. *See* Markoff, *supra* note 135 (describing researchers' efforts in creating an improved version of the Internet).

140. Zarsky, *supra* note 111, at 1026 (describing pure anonymity as use of "disposable, one-time identities that cannot be traced back to [one's] actual [self]").

141. *See id.* at 1033.

142. *See* Froomkin, *supra* note 112, at 414–17 (comparing traditional and online forms of pseudonymous communication).

143. *See supra* notes 87–110 and accompanying text. The use of personal information to help determine college admissions or to aid in a company's hiring process is common.

144. *See supra* notes 87–94 and accompanying text.

145. Zarsky, *supra* note 111, at 1036 ("With pseudonymity, there will be fewer opportunities to abuse personal information, as a user can control the availability of potentially abusive information by ensuring that such information can be linked only to one dimension of his or her persona."). While murder resulting from misused personal information is thankfully rare, see *supra* note 98 and accompanying text, undisclosed personal information is used (and abused) to help inform decisions regarding college admissions, employee hiring, and even jury selection. *See* Amy Hockert, *Employers Use "Facebook" and "MySpace" to Weed Out Applicants*, FIRSTCOASTNEWS.COM, Sept. 8, 2006, http://www.wtlv.com/tech/news/news-article.aspx?storyid=64453; Jamila A. Johnson, *Voir Dire: To Google or Not to Google*, LAW TRENDS & NEWS, Fall 2008, http://www.abanet.org/genpractice/newsletter/lawtrends/08_fall/litigation_johnson.html.

The degree to which pseudonymity mitigates interference with autonomy depends upon each user's preference. Users who opt to only use one online pseudonym would not mitigate the harm at all.[146] At the other extreme, individuals who choose to use a persona only a few times before discarding it may completely eliminate these harms, but in doing so they necessarily forgo all online relationships.[147] Other users would fall somewhere in the middle, using one persona for professional activities, another for friends and family, and a handful of others for shopping, online games, and blogging. By separating out different aspects of one's life in this fashion, each user can choose the correct balance between privacy and the benefits afforded by the data collection industry—conveniences such as improved search engine results and pertinent advertisements.[148] If a user determines that the persuasive power of targeted advertising is too great, she can always begin again with a clean slate by abandoning one pseudonym in favor of another.[149]

Not only does pseudonymity serve to protect individual autonomy, it also allows one to seek out her identity.[150] Robust information privacy protection in the form of pseudonymity allows an individual to decide what aspects of her identity she wishes to disclose when forming online relationships. In this manner, the user becomes free to present herself—and view herself—however she chooses.[151] In terms of Giddens's "biographies," pseudonymity gives an individual the freedom to explore particular aspects of her identity, and possibly rewrite her biography, without negatively affecting her real-space or other online relationships.[152]

---

146. *See* Zarsky, *supra* note 111, at 1037 ("[E]very user . . . will be subject to several feedback loops, depending on the number of aliases he or she uses.").

147. *Cf.* Froomkin, *supra* note 112, at 423 (comparing anonymous and pseudonymous personas, and noting that the latter "allow for continuity of identity to be maintained over a period of time").

148. *See* Solove, *supra* note 9, at 506–11 (discussing privacy concerns regarding aggregation of personal information).

149. With respect to personal data collection, anonymity prevents the aggregation of personal information, whereas pseudonymity would permit controlled aggregation of private data. Zarsky, *supra* note 111, at 1038 ("[W]hen a user grows tired of a specific virtual personality, or is unhappy with the feedback it generates, he or she can simply set it aside.").

150. *See* SACO, *supra* note 2, at 120 (describing "cyberspace as a different kind of social space: one for the exploration and development of new and different senses of self"); Jerry Kang, *Cyber-Race*, 113 HARV. L. REV. 1130, 1206 (2000) (arguing that the Internet's promise of "liberation and equality" is naïve, but that through "racial pseudonymity" the lines that separate races and genders may "slowly dissolve" to provide more freedom).

151. *But see* Jodi O'Brien, *Writing in the Body: Gender (Re)production in Online Interaction*, *in* COMMUNITIES IN CYBERSPACE 76, 99 (Marc A. Smith & Peter Kollock eds., 1999) (noting that although it is possible to "mentally transgender or ungender oneself in one's own imagination," it does not follow that "an institutionalized gender binary—and its consequences—will necessarily cease to exist. Rather the act of transgressing the binary may in fact reinscribe it.").

152. *See* Sarah Nettleton et al., *The Reality of Virtual Social Support*, *in* VIRTUAL SOCIETY?: TECHNOLOGY, CYBERBOLE, REALITY 176, 187 (Stevel Woolgar ed., 2002) (describing how online pseudonymous social support may "contribute to ontological

Pseudonymity, in tandem with the various methods of interaction available through the Internet, can be extremely valuable to individuals seeking ways to escape any stigmas, prejudices, or real-world reputational baggage—i.e., it provides users with a clean slate and an opportunity to socialize on the individual's own terms.[153]

Online anonymity and pseudonymity can also facilitate antisocial behavior. The lack of accountability enjoyed by anonymous users not only shields expressive speech but gives rise to "trolls"—users who intentionally "antagonize others [online]" through harmful, negative comments and behavior.[154] Pseudonymous users are also freer to express negativity and deceive others, though often at the cost of reputational capital.[155] In one incident that attracted great attention from the press, a thirteen-year-old girl with "a history of depression and suicidal impulses" took her own life after being the target of a cyber-bully on the social networking website MySpace.[156] Ultimately, little can be done to prevent this type of behavior, though traceability, community norms, and code—i.e., the architectures of the Internet and the specific mode of interaction—mitigate its prevalence.[157]

The second type of benefit that online pseudonymity provides is the creation of trusted online communities, often with fundamentally different

---

security whereby individuals have to create and recreate their biographies, and can reflect upon them in the light of the reactions and experiences of others").

153. LESSIG, *supra* note 123, at 86–87 (describing how "the blind, the deaf, and the 'ugly'"—three classes of people "disabled" in real-life—were made equal through pseudonymous communication).

154. Todd Leopold, *#@*!!! Anonymous Anger Rampant on Internet*, CNN.com, Nov. 3, 2008, http://www.cnn.com/2008/TECH/11/03/angry.internet/index.html; *see also* Danielle Keats Citron, *Cyber Civil Rights*, 89 B.U. L. REV. 61, 62–65 (2009) (recounting various "civil rights violations" facilitated by online anonymity, as "in practice, [anonymous online mobs] overwhelmingly target members of traditionally subordinated groups, particularly women").

155. *See* Mattathias Schwartz, *Malwebolence*, N.Y. TIMES, Aug. 3, 2008, at MM24 (discussing, *inter alia*, a lawsuit filed by two female Yale Law students "against pseudonymous users who posted violent fantasies about them on . . . a college-admissions message board").

156. Jennifer Steinhauer, *Woman Found Guilty in Web Fraud Tied to Suicide*, N.Y. TIMES, Nov. 27, 2008, at A25.

157. *Cf.* Kevin Poulsen, *MySpace Predator Caught by Code*, WIRED, Oct. 16, 2006, http://www.wired.com/science/discoveries/news/2006/10/71948 (traceability deters crime); *see* Elizabeth Reid, *Hierarchy and Power: Social Control in Cyberspace*, *in* COMMUNITIES IN CYBERSPACE, *supra* note 151, at 107, 114 ("The tendency toward disinhibition and the accompanying threat of anti-social behavior can be countered by an encouragement of uninhibited sociality. The apparent safety of anonymity encourages users to be expressive, which enmeshes them into a web of relationships."); *id.* at 107, 114–18 (describing antisocial behavior on MUDs and technological means to counteract such action); *see also* Nettleton et al., *supra* note 152, at 186 (describing the effects of antisocial flamers and noting that members of online communities surveyed considered such antisocial behavior to be the cost of pseudonymity—a cost worth paying, as "[t]he advantages far outweigh the disadvantages").

norms.[158] Pseudonymous users are able to express themselves freely, without the need for social niceties.[159] The Internet's capability for many-to-many interactivity—overcoming problems of collective action[160]—while providing everyone with the protections of pseudonymity, creates a unique social environment.[161] When combined with freedom of self-redefinition, the results can be quite remarkable.

Scholars have noted several emergent characteristics of these pseudonymity-facilitated relationships and communities. First, users interacting through pseudonymous personas often exhibit decreased inhibition,[162] which often leads to increased intimacy and strong personal relationships.[163] These relationships may permit individuals to extend their social networks, at times providing invaluable social support.[164] Particularly those with "concealable stigmatized identities," for example, those who do not conform to socially accepted standards of gender or sexuality, benefit from such social support, often attaining a greater sense of self-acceptance.[165] However, even for the average user,

---

158. LESSIG, *supra* note 123, at 218 ("We all desire to live in separate communities, or among or within separate normative spaces. Privacy . . . supports this desire. It enables these multiple communities and disables the power of one dominant community to norm others into oblivion."); Susan E. Watt et al., *How Social Is Internet Communication?: A Reappraisal of Bandwidth and Anonymity Effects*, *in* VIRTUAL SOCIETY?: TECHNOLOGY, CYBERBOLE, REALITY, *supra* note 152, at 61, 68 ("[Pseudonymous] conditions in which individuating cues are reduced or eliminated produce *normative* behaviour.").

159. Nettleton et al., *supra* note 152, at 185 ("[T]he medium of exchange itself facilitates support—the [pseudonymity] in particular. Unlike other forms of interaction, one can 'dive straight in' . . . .").

160. *See infra* notes 168–78 and accompanying text.

161. *Cf.* Watt et al., *supra* note 158, at 68 (summarizing "two recent meta-analyses of nearly 100 studies of anonymity . . . , which concluded that group performance depends on the interaction between specific social context and relevant social norms and system characteristics such as anonymity").

162. One scholar suggests that this disinhibition is due, at least in part, to the freedom to discuss negative problems without fearing any repercussions to real-life relationships. Nettleton et al., *supra* note 152, at 184. Since generally such negative talk is limited to close relations—as they reveal "negative aspects of the self"—the norms which permit such talk also foster the creation of close, supportive relationships. *Id.*

163. Reid, *supra* note 157, at 112–13; *see also* Barry Wellman & Milena Gulia, *Virtual Communities as Communities: Net Surfers Don't Ride Alone*, *in* COMMUNITIES IN CYBERSPACE, *supra* note 151, at 167, 178–81 (measuring the strength of online relationships).

164. Nettleton et al., *supra* note 152, at 181 ("[T]he opportunity to extend their social network was invaluable. This was especially so for those who were socially isolated because of their geographical location, disability, or social circumstances."); *see id.* at 178 (defining "social support" and its effects).

165. Watt et al., *supra* note 158, at 61–62 ("[P]eople with concealable stigmatized identities (for example, being gay or holding extreme political beliefs) gain so much support from belonging to Internet groups that their self-acceptance increases, as does their likelihood of 'coming out' or letting other people know about their hidden self." (citations omitted)); Steve Silberman, *We're Teen, We're Queer, and We've Got E-mail*, WIRED.COM, Nov. 1994, http://www.wired.com/wired/archive/2.11/gay.teen_pr.html.

online relationships can often be as deep and meaningful as real-space relationships.[166] Thus, at least for some individuals, pseudonymity performs the dual function of granting the user the freedom to explore her identity while also facilitating the formation of online communities, providing invaluable social support and further aiding in the search for self.[167]

Online communities also provide a means for the efficient pooling of ideas, leading to cooperation on a massive scale.[168] This phenomenon has been the driving force behind the success of the Open Source Movement,[169] Creative Commons,[170] and wiki[171] sites such as Wikipedia.[172] Examples of open source software include the Linux operating system, the Apache Web Server (the most popular web serving software), and the web browser Mozilla Firefox.[173] As a rule,

166. *See* Karen A. Cerulo, *Reframing Sociological Concepts for a Brave New (Virtual?) World*, 67 SOC. INQUIRY 48, 50–54 (1997) (explaining that online relationships can be just as "real" as in real-life); *see also* Regina Lynn, *Don't Dismiss Online Relationships as Fantasy*, WIRED, Sept. 7, 2007, http://www.wired.com/culture/lifestyle/commentary/sexdrive/2007/09/sexdrive_0907; Nettleton et al., *supra* note 152, at 181.

167. *See* Nettleton et al., *supra* note 152, at 187 (noting that one of the benefits of online support is the opportunity it gives to individuals "to create and recreate their biographies, and can reflect on them in the light of the reactions and experience of others").

168. HOWARD RHEINGOLD, THE VIRTUAL COMMUNITY: HOMESTEADING ON THE ELECTRONIC FRONTIER 109 (2000) (describing this as a "rediscover[y] [of] the power of cooperation . . . [and] a merger of knowledge capital, social capital, and communion").

169. *See* Kris Frieswick, *Are Business Method Patents a License to Steal?*, CFO.COM, Sept. 2001, http://www.cfo.com/article.cfm/3000625.

170. Creative Commons is a nonprofit corporation providing free copyright "licenses and other legal tools to mark creative work with the freedom the creator wants it to carry, so others can share, remix, use commercially, or any combination thereof." About: Creative Commons, http://creativecommons.org/about/ (last visited Jan. 18, 2009). Professor Lessig's book *Code 2.0*, *supra* note 123, is the result of online collaboration and has been released under a Creative Commons license. Codev2: Lawrence Lessig, http://codev2.cc/ (last visited Jan. 19, 2009).

171. "A Wiki enables documents to be authored collectively in a simple markup language using a web browser. 'Wiki wiki' means 'super fast' in the Hawaiian language, and it is the speed of creating and updating pages that is one of the defining aspects of wiki technology." AssessNet Glossary, http://www.assessnet.org.uk/mod/glossary/view.php?id=625&mode=&hook=ALL&sortkey=&sortorder=&fullsearch=0&page=18 (last visited Mar. 30, 2009).

172. "Wikipedia is a free, multilingual encyclopedia project . . . . Wikipedia's 12 million articles (2.8 million in the English Wikipedia) have been written collaboratively by volunteers around the world, and almost all of its articles can be edited by anyone who can access the Wikipedia website. Launched in January 2001 . . . , it is currently the most popular general reference work on the Internet." Wikipedia, http://en.wikipedia.org/wiki/Wikipedia (last visited Mar. 30, 2009) (citations omitted). *See* LESSIG, *supra* note 123, at 243 (describing Wikipedia as "most extraordinary collaborative process" which has created "perhaps the most useful encyclopedia ever written").

173. *See* The Open Source Definition (Annotated), Open Source Initiative, http://www.opensource.org/docs/definition.php (last visited Nov. 7, 2008).

open source software is freely distributed, both in terms of alienability and price.[174] Although the collaboration is made possible by the many-to-many communication capabilities of the Internet, pseudonymity is often a key ingredient to foster this collaborative spirit.[175] This is particularly true when unpopular or contentious views are espoused—situations in which "a shield from the tyranny of the majority" is most needed.[176] The combination of collaboration, free-flowing ideas, and unfettered speech create the potential for a more participatory, rich, and direct democracy.[177] Pseudonymity provides benefits to individuals and online communities, both of which can have far-reaching effects upon our real-space societies.[178]

D. The Scope and Content of a Right to Pseudonymity

Given the many privacy-related and other benefits of pseudonymity, the Internet should retain and improve its ability to facilitate pseudonymous interactions. This section highlights several of the most important rights and legal protections that this author believes would strike the ideal balance between the competing, albeit at times overlapping, interests, which include: government's interest in enforcing laws; individuals' varied interests, each choosing her own balance of privacy and convenience; individuals' interest in exercising free expression; and data brokers' interest in generating profit. The section concludes with a more theoretical discussion of what a "right to pseudonymity" may entail in the future.

Before continuing, however, it may help to describe the identity management technology likely to be used to facilitate these pseudonymous interactions, known as Identity 2.0.[179] Imagine a single login which allows access to an individual's entire portfolio of anonymous, pseudonymous, and real-space

---

174. *See* Allen K. Yu, *Enhancing Legal Aid Access Through an Open Source Commons Model*, 20 HARV. J.L. & TECH. 373, 376–79 (2007) (describing the origins and ethics of the open source movement).

175. David Post advocates for the protection of pseudonymous communication specifically to "induce 'investors' to pool their intellectual capital" into these collaborative communities. Post, *supra* note 119, at 160; *see* Nettleton et al., *supra* note 152, at 183–84 (describing "informational support" in the context of pseudonymous support groups as the "most readily obvious source of social support on the internet").

176. McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 357 (1995) (citing J. MILL, ON LIBERTY AND CONSIDERATIONS ON REPRESENTATIVE GOVERNMENT 1, 3–4 (R. McCallum ed., 1947)) ("Anonymity is a shield from the tyranny of the majority.").

177. *See, e.g.*, Police Act Review Wiki, http://wiki.policeact.govt.nz/wiki/ (last visited Feb. 20, 2009) (collaborating to draft a new Policing Act for New Zealand in 2007—enacted in 2008). Exactly how much democracy is benefiting and will benefit from the Internet is a highly contentious issue.

178. Nettleton et al., *supra* note 152, at 176 ("[T]here exists a strong relationship between levels of *social capital* and *social support*, on the one hand, and levels of health and well-being on the other."); *id.* at 177 ("[H]ow we both experience and provide social support is changing."); *see* Post, *supra* note 119, at 163.

179. *See* Jeffrey Aresty, *Digital Identity and the Lawyer's Role in Furthering Trusted Online Communities*, 38 U. TOL. L. REV. 137, 153 (2006) (describing Identity 2.0).

identity profiles.[180] Once a user proves who she is, authenticated by an "identity provider," the user is able to create and manage various identity profiles—e.g., single-use anonymous profiles, enduring pseudonymous profiles, and a profile based on the user's real-space identity.[181] In this fashion, the user is able to decide what personal information is associated with each profile—information like her age, contact information, and nationality.[182] "Resource providers" like eBay, Amazon, and blogging websites that ask for personal information are thus able to verify that the user is who she says she is, but without ever knowing her real-space identity, unless she chooses to disclose that information.[183] Furthermore, a resource provider cannot combine personal data collected from multiple pseudonymous profiles owned by the same user, giving users maximum control over their information privacy.[184]

1. General Nontraceability

The online pseudonymity discussed above was "untraceable." However, governments are unlikely to permit untraceable pseudonymity, due to their strong interest in maintaining order and enforcing civil and criminal laws.[185] The privacy-related benefits of online pseudonymity may still be enjoyed to a lesser degree if pseudonyms are made traceable. The benefits decrease, however, as the perceived likelihood of tracing increases. For this reason, a legally enforceable "right to not-be-traced" will minimize the actual and perceived likelihood of tracing, such that individuals stripped of their pseudonymous protections are entitled to some meaningful amount of compensation.

This right not-to-be-traced arises from three distinct relationships and the rights that derive from them. First and foremost, there is the fiduciary relationship

---

180. The login could include biometrics—such as a retina scan, a password-protected portable computer such as an iPhone, or other forms of identification. *See, e.g.*, Thibault Candebat & David Gray, *Secure Pseudonym Management Using Mediated Identity-Based Encryption*, 14 J. COMPUTER SEC. 249, 249 (2006) (discussing an identity management scheme using mobile phones).

181. *See* Dick Hardt, *ETech 2006: Who Is the Dick on My Site?*, http://identity20.com/media/ETECH_2006/ (downloadable video) (last viewed Jan. 17, 2009).

182. *Id.*

183. *Id.*

184. *See* Zarsky, *supra* note 111, at 1034–35 (describing pseudonymity as creating two "walls," separating the real-space identity from its pseudonyms and separating pseudonymous personas from each other); SOLOVE, *supra* note 1, at 44–47 (discussing the "aggregation effect" of personal data collection). *But see* Monica Chew et al., Google, Inc., *(Under)mining Privacy in Social Networks*, at 1, http://w2spconf.com/2008/papers/s3p2.pdf (describing "three distinct areas where the highly-interlinked world of social networking sites can compromise user privacy" as "(1) lack of control over activity streams; (2) unwelcome linkage; and (3) deanonymization through merging of social graphs") (last visited Feb. 19, 2009).

185. *See* Privacy International, *The UN Internet Governance Forum and Privacy*, Dec. 18, 2007, http://www.privacyinternational.org/article.shtml?cmd[347]%3C/a%3E=x-347-559087&als[theme]=Privacy%20and%20Human%20Rights (discussing U.N. Internet Governance Forum summits' overall emphasis on "cyber-security" and "war on terrorism").

between the user and the identity provider.[186] If the identity provider negligently leaks a user's personal information, that user's entire portfolio of profiles becomes compromised. To deter such negligence and compensate the user, both statutory and compensatory damages should be available.

Second is the relationship of trust between users and government, which must be able to trace pseudonyms to their real-space identities to enforce civil and criminal laws. Yet for individuals and society to enjoy the privacy-related and other benefits of pseudonymity, the government must assure users that it will not pierce the pseudonymous veil without due process of law.[187] Such a system will permit users in oppressive regimes to speak freely without fear of reprisal.[188] The need for robust procedural protections is illustrated by the prevalence of frivolous online defamation lawsuits initiated by parties solely to discover—and ultimately silence—the real-space identity of their pseudonymous critics.[189]

Third is the multitude of relationships between a user and other private individuals. Security of personal information in the previous two relationships, including ownership of pseudonymous personas, is largely a function of the proper use of technology—literally a right to not be traced. Regulating the sharing of private information between individuals, on the other hand, has profound First Amendment implications. The U.S. Constitution and First Amendment jurisprudence jealously guard an individual's right to speak the truth about others,

---

186. *Cf.* SOLOVE, *supra* note 1, at 103 ("[T]he law should hold that companies collecting and using our personal information stand in a fiduciary relationship with us.").

187. This right derives from the procedural due process rights guaranteed by the Fourteenth Amendment of the U.S. Constitution. *See also infra* notes 195–99 and accompanying text (analogizing pseudonyms to corporations).

188. *See* Kenneth Denby, *Bloggers Who Risked All to Reveal the Junta's Brutal Crackdown in Burma*, TIMES ONLINE, Oct. 1, 2007, http://www.timesonline.co.uk/tol/news/world/asia/article2563937.ece.

189. *See* CyberSLAPP Information Page, http://www.cyberslapp.org/ (last visited Jan. 17, 2009). In consonance with the idea that the identity of Internet users deserves robust procedural protection, the Maryland Supreme Court recently held:

> [W]hen a trial court is confronted with a defamation action in which anonymous speakers or pseudonyms are involved, it should, (1) require the plaintiff to undertake efforts to notify the anonymous posters that they are the subject of a subpoena or application for an order of disclosure, including posting a message of notification of the identity discovery request on the message board; (2) withhold action to afford the anonymous posters a reasonable opportunity to file and serve opposition to the application; (3) require the plaintiff to identify and set forth the exact statements purportedly made by each anonymous poster, alleged to constitute actionable speech; (4) determine whether the complaint has set forth a prima facie defamation per se or per quod action against the anonymous posters; and (5), if all else is satisfied, balance the anonymous poster's First Amendment right of free speech against the *strength* of the *prima facie* case of defamation presented by the plaintiff and the necessity for disclosure of the anonymous defendant's identity, prior to ordering disclosure.

Indep. Newspapers, Inc. v. Brodie, 966 A.2d 432, 457 (Md. 2009).

except in very limited situations.[190] As a result, a user who shares the existence of a pseudonymous profile with another individual should generally have no legal recourse when the individual discloses that information to others. An important exception to this rule is that a natural or juridical person who obtains the information through misrepresentation or discloses such information for profit could be held liable for the disclosure.[191] Therefore, if a user wants privacy, she should keep her pseudonymous personas private.

2. Pseudonymous Reputation

A user whose pseudonymous persona is defamed should be able to bring suit in certain instances to protect the persona's reputation.[192] Additionally, if a pseudonymous profile becomes sufficiently famous, the reputation accrued by the pseudonym could receive legal protection under trademark law.[193] Presumably, individuals could be prevented from using pseudonyms identical or similar to well-known pseudonyms in a similar field of business. For example, if a pseudonymous blogger named "Digital Cameron" blogged about digital cameras and received some income from advertisements placed on the blog, he may be able to enjoin someone from coming along and creating a competing digital camera blog under the name "Digital Cameroon." Other trademark claims, such as dilution by blurring and tarnishment, would also apply to protect the goodwill in a pseudonym.[194]

3. Rights of Pseudonymous Personas

The aforementioned rights all belong to the real-space owner of the pseudonymous persona. This final subsection discusses the possibility of recognizing a pseudonymous persona as a legal entity, and the repercussions flowing therefrom.

Pseudonymous personas function similarly to corporations: while a corporation limits liability in the legal sense, a pseudonym protects the reputations

---

190. *See* SOLOVE & ROTENBERG, *supra* note 10, at 102–59.

191. *Cf.* Cent. Hudson G&E Corp. v. Pub. Serv. Comm'n N.Y., 447 U.S. 557, 562–65 (1980) (granting less protection and applying intermediate scrutiny to commercial speech).

192. David R. Johnson & David G. Post, *Law and Borders—The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367, 1402 (1996) ("A user's claim to a right . . . to redress when [her online] identity's reputation suffers harm, may be valid even if that identity does not correspond exactly to that of any single person in the real world."); *see also* Joseph Blocher, *Reputation as Property in Virtual Economies*, 118 YALE L.J. POCKET PART 120, 124–25 (2009) ("The major task for future scholarship about reputational economies is to determine if these reputational norms are clear and enforceable, and whether and how they should be backed by formal rules.").

193. *Cf.* Ji v. Bose Corp., 538 F. Supp. 2d 349, 351–52 (D. Mass. 2008) (granting summary judgment for defendant where plaintiff could not show she was sufficiently well-known to satisfy the "level of recognition" factor of the eight-factor test for a false endorsement claim).

194. Trademark Dilution Revision Act, 15 U.S.C. § 1125(c) (2006).

of its owner or owners, thus providing reputational "limited liability."[195] The act of tracing a pseudonymous persona back to its real-space owner is analogous to piercing the corporate veil, stripping the entity of its liability-limiting characteristic and allowing for a balance of protection and accountability.[196]

Following this parallel to its logical next step, we must ask whether the law should recognize pseudonymous personas as legal entities—complete with rights and duties, including the right to sue. Professor Post argued over a decade ago that pseudonymous personas should be granted legally recognized status, including the right to sue, due to the benefits that they confer.[197] If pseudonymous personas are ever granted legal rights, they may gain economic value beyond that of trademarks, such that they will be transferred and sold. Furthermore, a pseudonym that is defamed could defend itself by bringing suit on its own behalf.[198]

III. PROCEDURAL DIFFICULTIES REGARDING A RIGHT TO PSEUDONYMITY

While market regulation of the personal data industry is a necessary first step to securing user privacy,[199] a strong privacy protection regime requires that individuals have some form of private right of action when the regulations are breached or ignored. Many scholars contend that adapting property or contract law may provide individuals with the legal recourse needed to secure their personal information.[200] While contractual or property rights may serve to protect personal information in many instances, this author believes that the protections afforded by tort law must also be brought to bear in order to provide comprehensive privacy protection on the Internet. Tort law will provide gap-filling default rules in situations not covered by other laws, just as it presently does in real-space.[201] With the Internet's global reach, meaningful privacy laws must be internationally enforceable. In addition to the need to harmonize the substantive law governing privacy on the Internet, effective enforcement of privacy rights online requires a method to reconcile various countries' procedural rules regarding personal jurisdiction and choice of law. This Part addresses these two important procedural problems and proposes a possible solution.

---

195. Post, *supra* note 119, at 160.

196. *See id.* at 161.

197. *See id.*

198. *See* Johnson & Post, *supra* note 192, at 1402.

199. *See supra* Part I.C.

200. *See, e.g.*, LESSIG, *supra* note 123, at 228–30 (abandoning his previous promotion of property-law model in favor of contractual model for protecting privacy); Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373, 1384–91 (2000) (examining usage restrictions within intellectual property licensing arrangements as a possible model for the propertization of personal information).

201. *See, e.g.*, Jessica Litman, *Information Privacy/Information Property*, 52 STAN. L. REV. 1283, 1311–13 (2000) (advocating for use of breach of trust tort to protect personal data); Andrew J. McClurg, *A Thousand Words Are Worth a Picture: A Privacy Tort Response to Consumer Data Profiling*, 98 NW. U. L. REV. 63, 69 (2003); Robert C. Post, *The Social Foundations of Privacy: Community and Self in the Common Law Tort*, 77 CAL. L. REV. 957, 959 (1989).

Most scholars agree that current procedural laws are often inadequate when applied to the Internet, resulting in jurisdictional uncertainty arising from the imposition of the geographically-based jurisdictional canon upon online activities.[202] However, some commentators continue to argue that the challenges posed by the Internet, while sizeable, are nonetheless surmountable.[203] This Part begins by demonstrating when and why jurisdictional and choice-of-law rules break down when applied to some Internet controversies but not others. It concludes with a possible solution to this procedural dilemma.

A. Cybertorts, Jurisdiction, and Choice of Law

Legal issues regarding online privacy not based in contractual agreements are particularly resistant to jurisdictional and choice-of-law rules. While the tortious conduct in these cases occurs in cyberspace, the harm is felt wherever the injured party resides in real-space. Thus, the only connections to geographic locations in these cases are the real-space locations of the tortfeasor and the injured party. Due to the ubiquity of pseudonymity on the Internet, the tortfeasor often has no idea where the injured party resides—making it difficult to justify subjecting the tortfeasor to the reach of the personal jurisdiction or substantive laws of the injured party's home forum.

To aid this discussion, it is necessary to distinguish between these torts that pose unique, arguably insurmountable challenges due to their relationship with cyberspace and those that do not. To this end, a new definition of the term "cybertort" is offered—namely, tortious conduct which, if the Internet were a separate jurisdiction for choice-of-law purposes, would be subject to the substantive law of the Internet.[204] For purposes of this Note, the applicable choice-of-law rules are those of the Second Restatement of Conflicts of Law[205]—though the definition remains equally viable for any contacts-counting choice-of-law analysis.[206]

The following hypothetical scenario serves primarily to illustrate the law's inability to protect online privacy in a just and effective manner. Additionally, it illustrates several privacy-related injuries that can result from

---

202. *See, e.g.*, LESSIG, *supra* note 123, at 302 ("When a large number of citizens live in two different places, and when one of those places is not solely within the jurisdiction of a particular sovereign, then what kinds of claims can these sovereigns make on cyberspace?").

203. *See generally* Frank H. Easterbrook, *Cyberspace and the Law of the Horse*, 1996 U. CHI. LEGAL F. 207 (1996) (disparaging the study of "cyberlaw" as a standalone subject).

204. The term "cybertort," as used in legal literature, seems to mean "a cause of action that exists due to harmful Internet contact." Daniel P. Schafer, *Canada's Approach to Jurisdiction over Cybertorts:* Braintech v. Kostiuk, 23 FORDHAM INT'L L.J. 1186, 1190 n.28 (2000) (citing Rosalind Resnick, *Cybertort: The New Era*, NAT'L L.J., July 18, 1994, at A1).

205. RESTATEMENT (SECOND) OF CONFLICTS OF LAW § 145 (1971).

206. For example, the Rome II Convention on the Law Applicable to Non-contractual Obligations provides for an exception to the traditional *lex loci delicti* choice-of-law rule if another country has a "manifestly closer connection" to the case. Council Regulation 864/2007, art. 4(3), 2007 O.J. (L 199) 40, 44 (EC).

online activities. The analysis focuses on the *locus actus*, or "place of the (tortious) act," and the *locus delicti*, or "place of the injury." Together, these two locations act as shorthand for modern choice-of-law rules in the United States, generally requiring application of the laws of the state "with the most significant relationship to the occurrence and the parties."[207] Additionally, the *locus actus* and *locus dilecti* generally determine which fora may assert personal jurisdiction over the tortfeasor.[208]

B. Hypothetical: Tortious Collection, Transmission, and Sale of Personal Data

Internet Marketing Research, Inc. (IMR) collects, analyzes, and sells personal information that it gleans from Internet users' online activities.[209] It gathers this information through agreements with a variety of websites, including those that offer online shopping, news, travel, and search engine capabilities.[210] IMR's privacy policy states that it may use the information gathered for marketing research purposes and may also use the information for any other purpose, "as permitted by law."[211]

IMR decides to sell a portion of the information they collect and the results of their analysis of the data to a detective agency, Cyber-Sleuths. IMR transmits the requested data to Cyber-Sleuths without employing any encryption methods.[212] Now, assume that any of the following activities could subject IMR to

---

207. RESTATEMENT (SECOND) OF CONFLICTS OF LAW § 145 (1971) ("Contacts to be taken into account . . . include: (a) *the place where the injury occurred*, (b) *the place where the conduct causing the injury occurred* . . . .") (emphasis added).

208. For example, in a standard online defamation case, the *locus actus* of the defamation is in cyberspace; the *locus delicti*, however, is the real-space location where the effects of the defamatory conduct are felt. *See* Bettina M. Chin, Note, *Regulating Your Second Life: Defamation in Virtual Worlds*, 72 BROOK. L. REV. 1303, 1329–46 (2007) (describing requirements for defamation claim in real-space and cyberspace). The harmful effects of online defamation alone, however, may not be enough to support the exercise of personal jurisdiction over the defendant. *See, e.g.*, Revell v. Lidov, 317 F.3d 467, 476 (5th Cir. 2002) (affirming district court holding that merely posting defamatory article on Internet results in insufficient "minimum contacts" to establish personal jurisdiction).

209. *See* Froomkin, *supra* note 112, at 479–505 (explaining how such information is used to create consumer profiles).

210. *See* Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609, 1621–32 (1999) (describing the various ways in which information is collected and distributed via the Internet); *see also* Daniel D. Barnhizer, *Propertization Metaphors for Bargaining Power and Control of the Self in the Information Age*, 54 CLEV. ST. L. REV. 69, 77 (2006).

211. The relevant question is: whose law is applicable? *Cf.* Chase Bank Privacy Policy, *available at* http://www.chase.com/privacy (last visited Feb. 26, 2009) ("You may tell us not to share information about you with non-financial companies outside of our family of companies. Even if you do tell us not to share, *we may do so as required or permitted by law*." (emphasis added)). Except for customers residing in California, the law offers only minimal protection. *See generally* Anthony D. Milewski Jr., *Compliance with California Privacy Laws: Federal Law Also Provides Guidance to Businesses Nationwide*, 2 SHIDLER J.L. COM. & TECH. 19 (2006).

212. *See* LESSIG, *supra* note 123, at 140–41 (describing why encryption is necessary to safeguard data).

civil liability: (1) collection of personal information without clearly describing the uses for the data;[213] (2) collection of personal information from minors;[214] (3) transmission of unencrypted personal data by entities that collect such data;[215] (4) transferral of personal data to third parties who do not meet certain minimum requirements for data security;[216] and (5) accessing personal data without permission from the collectors of that data or from those from whom the data were originally collected.[217]

Assuming IMR engaged in or permitted each of these tortious[218] activities to occur, the *locus actus* of some of these activities could arguably be stretched to some real-space location, such as the location of the servers.[219] However, determining jurisdiction or choice of law based upon the location of servers is an approach that has been rejected by the courts—and one which could readily be manipulated to minimize liability.[220] The simpler, more logical conclusion is to declare the *locus actus* of IMR's acts to be cyberspace. The *locus delicti* of any economic harm that would flow from the unlawful conduct would be the real-space location where the injured party happened to reside at the time.[221] The *locus delicti* of any privacy-related harm, according to standard jurisdiction and choice-of-law analyses, would also be the injured party's real-space location—as any harm to an individual's privacy or pocketbook necessarily occurs where that individual is located. Whether such harm would be enough to subject IMR to specific personal jurisdiction in any U.S. forum is an open question, requiring a thorough analysis of the facts.[222] If personal jurisdiction is established, the forum's

---

213. *See* Council Regulation 45/2001, art. 5(d), 2001 O.J. (L 8) 1, 5–6 (EC) ("Personal data may be processed only if . . . the data subject has unambiguously given his or her consent.").

214. *See* Children's Online Privacy Protection Act of 1998, 15 U.S.C. § 6501–6506 (2006) (prohibiting online service providers from knowingly collecting personal information from children under thirteen).

215. *See* Council Regulation 45/2001, art. 9, 2001 O.J. (L 8) 1, 7.

216. *See id.*; Michael L. Rustad & Thomas H. Koenig, *Negligent Entrustment Liability for Outsourced Data*, J. INTERNET L., Apr. 2007, at 3, 3–4.

217. *See* Council Regulation 45/2001, art. 22, 2001 O.J. (L 8) 1, 12–13. There is theoretical support for this tort in U.S. tort law, such as the tort of Intrusion to Seclusion. RESTATEMENT (SECOND) OF TORTS § 652B (1977).

218. While some of these jurisdictional and choice-of-law issues may be avoided by scrupulous use of contractual agreements, this does not address infractions by third parties, who would be without contractual privity.

219. The collection of personal information probably occurs on one or more of IMR's servers. The transmission of such information might be deemed to occur in two places: the source and destination of such information.

220. *See* American Bar Association Global Cyberspace Jurisdiction Project, *Achieving Legal and Business Order in Cyberspace: A Report on Global Jurisdiction Issues Created by the Internet*, 55 BUS. LAW. 1801, 1843–44, 1909 (2000) ("[A] server could be anywhere, and, indeed, as a result of mirror sites, the web site could be 'located' in several places at once.").

221. *Cf.* Calder v. Jones, 465 U.S. 783, 789 (1984) (establishing the effects doctrine).

222. A court would apply the two-part test for personal jurisdiction, first asking whether there are sufficient "minimum contacts" to exercise jurisdiction, then applying a

court will most likely apply its own substantive laws to the case, as it is unlikely that another jurisdiction will be found to have a "more significant relationship" when the real-space contacts are already so tenuous.[223] Thus, if the only jurisdiction willing to assert personal jurisdiction over IMR is its place of incorporation, then a plaintiff's right of action is limited to only those activities prohibited by the laws of IMR's home jurisdiction.

C. A New Paradigm for Old Procedural Rules

Scholars have suggested many possible changes and improvements to the current jurisdictional and choice-of-law rules as they apply to the Internet. Proposals include such varied approaches as an Internet governed by self-regulation,[224] new domestic courts or arbitral bodies with jurisdiction over Internet-based controversies,[225] and a variety of treaty-based approaches.[226] Although Internet self-regulation may be a viable solution to many of the challenges that cybertorts pose, total autonomy from real-space governments is unlikely to become a reality, as it would require all governments to allow the Internet to secede from their jurisdictions. No government will agree to this solution anytime soon.[227] Introducing new courts or arbitration tribunals may speed the law's ability to address the legal challenges posed by the Internet, but they are no solution in and of themselves. Finally, although scholars have proposed many international treaties and methods for harmonization, thus far none have addressed these challenges in a satisfactory manner.

---

separate fairness analysis. Asahi Metal Indus. Co. v. Superior Court, 480 U.S. 102, 109 (1987).

223. RESTATEMENT (SECOND) OF CONFLICTS OF LAWS § 145 (1971); *see also* Mut. Serv. Ins. Co. v. Frit Indus., 358 F.3d 1312, 1321 (11th Cir. 2004).

224. *See* Johnson & Post, *supra* note 192, at 1379 (advocating for self-regulation of online communities, with a distinct "law of Cyberspace" to be determined by those who populate the Internet); *see also* Jennifer L. Mnookin, *Virtual(ly) Law: The Emergence of Law in LambdaMOO*, 2 J. COMPUTER-MEDIATED COMM. (SPECIAL ISSUE) (1996), http://jcmc.indiana.edu/vol2/issue1/.

225. *See, e.g.*, Henry H. Perritt, Jr., *Jurisdiction in Cyberspace*, 41 VILL. L. REV. 1, 93–103 (1996) (proposing international arbitration or U.S. District Court for Cyberspace as possible solutions to jurisdictional problems of online civil controversies); Georgios I. Zekos, *State Cyberspace Jurisdiction and Personal Cyberspace Jurisdiction*, 15 INT'L J.L. & INFO. TECH. 1, 36–37 (2007) (arguing for establishment of "[c]yber courts and cyber arbitral tribunals" that would "have jurisdiction to solve all actions taking place on the net" and for "universal cyberspace jurisdiction" for all real-space courts where "electronic transactions have the potential to affect simultaneously all [real-space] jurisdictions").

226. *See, e.g.*, Michael L. Rustad & Thomas H. Koenig, *Harmonizing Cybertort Law for Europe and America*, 5 J. HIGH TECH. L. 13, 53–56 (2005) (describing methods to address procedural difficulties posed by Internet, including adoption of international treaties).

227. Such demands for treating the Internet as a self-regulating jurisdiction generally accompanied the arguments that the Internet was a separate place which could not be governed by the laws of real-space governments. *See* STUART BIEGEL, BEYOND OUR CONTROL?: CONFRONTING THE LIMITS OF OUR LEGAL SYSTEM IN THE AGE OF CYBERSPACE 25–49 (2001). Given that the current consensus is that cyberspace *is* in fact highly regulable, these calls for self-regulation have lost their momentum.

This author offers the following set of jurisdictional and choice-of-law rules as a possible solution to some of the current procedural difficulties inherent in civil controversies centered on the Internet. These rules can be modified and incorporated into a treaty to create a more predictable and just rule of cyberlaw. Adapting these same rules may also resolve conflicts between states within the United States.

For the sake of simplicity, this discussion assumes that these procedural rules are part of a multilateral treaty on torts in cyberspace, though the rules are just as easily incorporated into other agreements or laws, such as bilateral treaties and U.S. federal legislation. First, the treaty must adopt a test that distinguishes between real-space torts and cybertorts.[228] If the controversy in question is a cybertort action, then the substantive and procedural rules set out in the treaty would apply. If not, then the treaty will not apply at all, permitting the default jurisdictional and choice-of-law rules of the forum to operate.[229] If the treaty applies, no choice-of-law question remains, as the substantive laws of the treaty govern the case. The treaty would necessarily specify various other related laws, such as the applicable defenses and statutes of limitations.[230]

There are two main alternatives in determining which courts could potentially have jurisdiction: (1) each state in which the plaintiff and defendant are domiciled; or (2) all signatory states to the treaty. Although the second may appeal viscerally to those who regularly inhabit the Internet, there are a few shortcomings of such a system—e.g., language and cultural barriers creating hardship for one or both parties. By limiting the potential fora to only those jurisdictions where the parties are domiciled, the probability of such hardship for one or both parties almost certainly decreases. Finally, forum non conveniens could always be incorporated into the treaty for use by a court to dismiss a case without prejudice. Thus, this author believes that a fair rule would grant personal jurisdiction to courts of general jurisdiction in the fora where either the plaintiff or defendant is domiciled. However, in situations where the plaintiff and defendant reside in the same jurisdiction, the local substantive and procedural laws of the forum should apply in lieu of the treaty, as no other forum has an interest in the case.[231]

---

228. *See supra* text accompanying note 204. This treatment of cybertorts is in consonance with the underlying basis for the Second Restatement's rationales for permitting application of the laws of a foreign jurisdiction—namely, the prevention of forum shopping and the recognition that a foreign State may have a stronger interest in having its laws applied.

229. In most cases, therefore, the primary controversy will be over the characterization of the cause of action as sounding in tort of either the traditional or cybertort variety.

230. *See* Marine Constr. & Design Co. v. Vessel Tim, 434 P.2d 683, 686–87 (Alaska 1967) (detailing the "'built-in' limitation exception to the general rule that the forum's period of limitations governs").

231. For a similar provision, see article 4(2) of the Rome II Convention on the Law Applicable to Non-contractual Obligations. Council Regulation 864/2007, art. 4(2), 2007 O.J. (L 199) 40, 44 ("[W]here the person claimed to be liable and the person sustaining damage both have their habitual residence in the same country at the time when the damage occurs, the law of that country shall apply.").

IV. A ROADMAP TO A RIGHT TO PSEUDONYMITY

Hopefully at this point, the reader is intrigued by (if not convinced of) the desirability of a right to pseudonymity described in Part II.D above. This Part addresses the challenges of and outlines the steps necessary to implement a right to pseudonymity in the United States.

A. Domestic Regulation of the Personal Information Market

As well-intentioned as Google and other data collectors may be, self-regulation of the personal information industry is not an option.[232] While many of the most visible online data collectors have begun to take steps to protect user privacy,[233] these steps are only a partial solution. Further, these steps are entirely voluntary.[234] Due to the opacity and pervasiveness of online data collection, many users are unaware of which parties are collecting what types of information, further compounding the problem.[235]

In addition to the practical need for greater privacy protections in the United States, there is also an economic impetus for the United States to take such measures. Many countries have begun to enact data privacy laws, in part to "ensure that trade will not be affected by the requirements" of EU law.[236] The reluctance of the United States to regulate the data collection industry has led to a compromise—upon threat of sanctions and the loss of international trade—in the form of the U.S.–EU Safe Harbor Agreement.[237]

---

232. Many scholars have called for such regulation. *See, e.g.*, Cohen, *supra* note 200, at 1437–38; Solove, *supra* note 101, at 1456; Sovern, *supra* note 34, at 1048–51.

233. For example, Google has recently provided users with "the ability to see and edit the information that it has compiled about their interests for the purposes of behavioral targeting" and also "give[s] users the choice to opt out." Miguel Helft, *Google to Offer Ads Based on Interests, with Privacy Rights*, N.Y. TIMES, Mar. 11, 2009, at B3. *See also supra* notes 38–43 and accompanying text (describing Google's "partial anonymization" of personal information).

234. *See id.*

235. *See infra* notes 240–46 and accompanying text.

236. SOLOVE & ROTENBERG, *supra* note 10, at 688 ("The EU Data Directive has had a profound effect on the development of privacy law, not only in Europe but also around the world."). The EU has been pressing the issue, which has led to a compromise in the form of the Safe Harbor Agreement between the United States and European Union.

237. Marsha Cope Huie et al., *The Right to Privacy in Personal Data: The EU Prods the U.S. and Controversy Continues*, 9 TULSA J. COMP. & INT'L L. 391, 395–402 (2002). The Safe Harbor Agreement "allows onward transfer of EU data to U.S. companies complying with Safe Harbor requirements." *Id.* at 397. *See generally* SOLOVE & ROTENBERG, *supra* note 10, at 735–63. For a discussion on the effects of the EU's privacy laws on the United States, see *The EU Data Protection Directive: Implications for the U.S. Privacy Debate: Hearing Before the S. Comm. on Commerce, Trade, and Consumer Prot. and the Comm. on Energy and Commerce*, 107th Cong. (2001) (statement of Joel Reidenberg, Professor of Law and Director of Graduate Program at Fordham University School of Law), *available at* http://reidenberg.home.sprynet.com/Reidenberg_Testimony_03-08-01.htm.

B. User Education

Technological and legal tools to protect user privacy are worthless without educated users who understand the privacy implications of their decisions both on- and offline. Many users of credit cards and search engines have at most a vague understanding of how their personal information is collected, used, and sold by these companies.[238] A necessary first step towards a right to pseudonymity requires increased user awareness and greater resource provider transparency.[239]

As an example, consider the data collection practices of the popular social networking site Facebook.[240] By signing up for an account on Facebook, a user grants the website "an irrevocable, perpetual, non-exclusive, transferable, fully paid, worldwide license . . . to use, copy, publish, stream, store, retain, publicly perform, . . . and distribute . . . for any purpose" all photographs and other content uploaded by her to her Facebook page.[241] When the user adds an innocuous-looking third-party application, such as a movie quiz or game,[242] she consents to allow the third party to access her photos and other personal information.[243] Even if she chooses not to add the application, third parties may still "access and share certain information about [her] with others in accordance with [her] privacy settings," so long as at least one member of her social network uses the third-party application.[244] Finally, deactivating a Facebook account does not remove any information from Facebook's servers, but only from general public access.[245]

C. Internet Architecture and Policy

While many groups are working on various identity management systems similar to Identity 2.0, these systems are far from complete.[246] Once complete, resource providers such as Facebook, Google, and Amazon may have little

---

238. *See* MARY MADDEN ET AL., PEW INTERNET & AMERICAN LIFE PROJECT, DIGITAL FOOTPRINTS: ONLINE IDENTITY MANAGEMENT AND SEARCH IN THE AGE OF TRANSPARENCY ii (2007), http://www.pewinternet.org/pdfs/PIP_Digital_Footprints.pdf (concluding that most Internet users are not concerned about, and do not take steps to limit, personal information available about themselves online).

239. While improvements in technology—such as P3P—may promote transparency, technology alone cannot educate users. *See* William McGeveran, Note, *Programmed Privacy Promises: P3P and Web Privacy Law*, 76 N.Y.U. L. REV. 1812, 1843 (2001) (discussing P3P, Platform for Privacy Preferences).

240. Facebook, Welcome to Facebook!, http://www.facebook.com/ (last visited Jan. 17, 2009). *See generally* Yasamine Hashemi, *Facebook's Privacy Policy and Its Third-Party Partnerships: Lucrativity and Liability*, 15 B.U. J. SCI. & TECH. L. 140 (2009) (describing Facebook's partnerships with third-party websites and potential legal ramifications).

241. Facebook, Terms of Use, http://www.facebook.com/terms.php (last visited Jan. 17, 2009).

242. *See* Facebook Application Directory, http://www.facebook.com/apps/ (last visited Jan. 17, 2009).

243. Facebook Privacy Policy, http://www.facebook.com/policy.php (last visited Jan. 17, 2009).

244. *Id.*

245. *Id.*

246. *See supra* notes 180–85 and accompanying text.

incentive to adopt this "identity layer" unless privacy laws are in place.[247] Furthermore, an identity layer can be implemented simply to minimize identity theft or as a foundation for a new, pseudonymous society. Internet policymakers need to realize that the Internet was not designed with privacy in mind and, as a result, the decisions they make with regard to the future architecture of the Internet (privacy-related and otherwise) will have profound implications for future societies.[248]

D. Recognizing the Need for an International Treaty

Creating rules to regulate the collection and processing of personal information is only one part of the legal changes that need to occur. Unenforceable laws are no protection at all. The governments of the world must come to agree that the present procedural rules are unsatisfactory in certain situations involving the Internet. Governments must discard their choice-of-law and jurisdictional rules—mere legal fictions at this point—in favor of a just system of adjudication and enforcement that comports with international minimum due process requirements.[249] We need a predictable and orderly rule of law, instead of the present chaos of juridical confusion. To this end, an international treaty incorporating the procedural rules set forth in Part III.C above should be enacted.

The creation of an effective international treaty poses its fair share of challenges.[250] However, the proposed international convention has a real possibility of being ratified by most, if not all, democratic nations for the following reasons.[251] First, the scope of this treaty is quite narrow, only seeking to create privacy protections for the Internet—a goal shared by many countries. In this way, it promotes the interests of the sovereign state by extending protection of its

---

247. *See* SOLOVE, *supra* note 1, at 115–19.

248. *See* Markoff, *supra* note 135, at WK1 (describing researchers' attempts to improve the Internet and noting that "[a] more secure network is one that would almost certainly offer less anonymity and privacy").

249. Choice-of-law scholar Robert Leflar advocated that five interests be considered to "assure a continuing reexamination of precedents, a readiness to lay aside old mechanical rules that turn out to be without support in the considerations or that contradict them . . . ." ROBERT A. LEFLAR, AMERICAN CONFLICTS LAWS, § 108 (3d ed. 1977). Although Leflar was referring to the mechanical application of the First Restatement's general rule of *lex loci delicti*, his list of considerations is appropriate here to highlight how the Second Restatement's choice-of-law methodology has become a legal fiction when applied to cybertorts. Leflar's five considerations, the first three of which are uniformly applicable to all cybertorts, are: "(A) predictability of results; (B) maintenance of interstate and international order; (C) simplification of the judicial task; (D) advancement of the forum's governmental interests; and (E) application of the better rule of law." *Id.* § 96.

250. LESSIG, *supra* note 123, at 293 ("Law, at least as it regulates international relations, is the product of extended negotiations. . . . It will require the nations of the world to come to a common understanding about this space and to develop a common strategy for dealing with its regulation.").

251. It is unlikely that countries like Myanmar and China would be willing to abide by such an international agreement when they are so hostile to the flow of information from within and without their borders. *See generally* REPORTERS WITHOUT BORDERS, *supra* note 128.

citizens to cyberspace where, without such a treaty, any such legal protections would be largely illusory. Additionally, much more ambitious international conventions, such as the Cybercrime Convention, have recently been proposed, with some degree of success.[252] When compared to such agreements, this modest proposal seems to stand a reasonable chance of being accepted. Finally, this treaty would be an excellent way to test this method of treating cyberspace as its own jurisdiction for choice-of-law purposes. It could act as a testing ground to iron out the problems that will necessarily arise before enacting this or a similar solution to the current regime's shortcomings regarding jurisdictional and choice-of-law rules.

CONCLUSION: LAW AS A DRIVING FORCE FOR ARCHITECTURE

Many commentators have lamented the death of privacy.[253] While they may be correct about the end result if the personal data market is left unchecked, privacy's passing is hardly inevitable. This Note set forth the steps which this author believes to be necessary to revive this ailing, fundamental right. These steps begin with an electorate and a government that understands the ramifications of the data collection industry's practices if left unregulated.

The need to protect information privacy is real, and it is growing. Lawmakers must come to understand that policy questions about "Net Neutrality" and Internet architecture are much more fundamental than they may at first appear. Whether anonymity and pseudonymity and other transient "features" of the Internet will be incorporated into future iterations of the Internet are pivotal decisions[254]—decisions that will either strengthen or hobble freedom of thought and self-actualization in this and other democratic nations.

This author hopes that the idea of a right to pseudonymity encourages the formulation of future laws and policies, as well as the creation and implementation of new technologies. While some of the ideas pertaining to a right to pseudonymity are theoretical, most are not. The harms from lack of privacy are real and escalating, and the technology to implement the solution is within our reach. But without laws to drive these changes, a right to pseudonymity will remain but a netizen's utopian ideal.

---

252. *See* Council of Europe, Convention on Cybercrime, Nov. 23, 2001, C.E.T.S. No. 185, *available at* http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm.

253. *See, e.g.*, Laura Mandanas, *Editor's Note: Privacy Is Dead*, REPORTER ONLINE, Mar. 13, 2009, http://reportermag.com/article/03-13-2009/editors-note-privacy-is-dead.

254. *See* LESSIG, *supra* note 123, at 155 ("[T]he most important lesson about law in cyberspace is the need for law to account for the regulatory effect of code.").