2012

Chain-Link Confidentiality

Woodrow Hartzog
Boston University School of Law

INFORMATION PRIVACY

CHAIN-LINK CONFIDENTIALITY

Woodrow Hartzog[*]

TABLE OF CONTENTS

I. INTRODUCTION 658

II. PROTECTING PRIVACY IN THE DIGITAL AGE 661
A. THE PROMISE IN EVOLVING CONFIDENTIALITY 668
B. THE POTENTIAL FOR PRIVITY ONLINE 675

III. THE CHAIN-LINK CONFIDENTIALITY APPROACH 681
A. THEORY 682
1. Obligations and Restrictions on the Use of Information 683
2. Similarly Binding Future Recipients 687
3. Perpetuation of the Contractual Chain 694
B. IMPLEMENTATION 696

IV. CONCLUSION 702

[*] Assistant Professor, Cumberland School of Law at Samford University; Affiliate Scholar, Center for Internet and Society at Stanford Law School. The author would like to thank Neil Richards, Dean Smith, Daniel Solove, Natasha Duarte, Will DeVries, Ryan Calo, Anne Klinefelter, Danielle Citron, Bradley Areheart, Christian Turner, and the Staff of the *Georgia Law Review*.

I. INTRODUCTION

One of the most difficult challenges to the preservation of online privacy is the protection of information once it is exposed to other people. Generally, individuals lose control of their personal information once they disclose it on the Internet. People do not "own" personal information in the traditional sense. Consequently, they are forced to rely upon the recipients of their information, such as websites, to keep it safe.

The law provides few meaningful opportunities for Internet users to protect their own personal information. The current privacy laws are too limited, subjective, or vague to effectively police the "downstream" use of information by third parties.[1] Yet, there is a growing consensus that information privacy must be protected,[2] including calls for a privacy "bill of rights."[3] The challenge is not just if—but how—to protect an individual's privacy on the Internet.

---

[1] *See generally* Neil M. Richards, *The Limits of Tort Privacy*, 9 J. TELECOMM. & HIGH TECH. L. 357 (2011) (highlighting the conflict between disclosure privacy and the First Amendment and proposing an alternative remedial scheme to minimize the conflict); Neil M. Richards & Daniel J. Solove, *Prosser's Privacy Law: A Mixed Legacy*, 98 CALIF. L. REV. 1887 (2010) (arguing that Professor William Prosser's approach unduly limits privacy, rendering it ill-equipped to adapt to the changing technological and social environment); Daniel J. Solove, *Conceptualizing Privacy*, 90 CALIF. L. REV. 1087 (2002) (proposing a new pragmatic approach to conceptualizing privacy to replace current theories that are "either too narrow or too broad").

[2] *See, e.g.*, Danielle Keats Citron, *Cyber Civil Rights,* 89 B.U. L. REV. 61, 66 (2009) (advocating the creation of a "viable cyber civil rights agenda" to combat the greater ease with which individuals can participate in socially destructive behavior and acts).

[3] *See, e.g.*, Commercial Privacy Bill of Rights Act of 2011, S. 799, 112th Cong. (2011) (proposing a regulatory framework designed to protect individuals' personal data); Brian Achohido, *White House Issues Historic Call for Privacy Bill of Rights*, USA TODAY, Mar. 16, 2011, http://content.usatoday.com/communities/technologylive/post/2011/03/white-house-issues-historic-call-for-privacy-bill-of-rights/1 (noting the Obama Administration's support for a privacy bill of rights to protect individuals while using the Internet); Katy Bachman, *Government Dept. Recommends 'Privacy Bill of Rights,'* ADWEEK (Dec. 16, 2010), http://www.adweek.com/news/technology/government-dept-recommends-privacy-bill-rights-104045 (reporting the Commerce Department's Internet Policy Task Force's recommendations for a privacy bill of rights); *see also Public Opinion on Privacy*, ELEC. PRIVACY INFO. CTR., http://epic.org/privacy/survey/ (last visited Apr. 11, 2012) (citing numerous studies that demonstrate public opinion in favor of privacy rights, including "a February 2002 Harris Poll [that] showed that 63% of respondents thought current law [to be] inadequate to protect privacy").

This Essay proposes a "chain-link confidentiality" approach to protecting online privacy. A chain-link confidentiality regime would contractually link the disclosure of personal information to obligations to protect that information as it is disclosed downstream. Unlike other online privacy regimes that focus on the private nature of information, this proposal focuses on specific obligations within the relationships, not only between the discloser of information and the initial recipient, but also between the initial recipient and subsequent recipients.

Many have dismissed confidentiality law as a viable remedy for online privacy harms because they view it as a "one-off" protection or as too restrictive in contexts where sharing information is encouraged or required.[4] Even advocates of confidentiality law recognize that it is limited in that it typically only binds the initial recipient of information.[5] The discloser of information usually has no remedy under confidentiality law against third parties that further disclose confidential information.[6] At first glance, online information seems particularly ill-suited to be protected by confidentiality law because of the overwhelming amount of people who use the Internet and the ease with which information is distributed. After all, there are an estimated 1.97 billion Internet users worldwide visiting over 255 million websites.[7] Yet, only directly connected parties can become confidants.

Confidentiality law need not be limited to the initial recipient of information, however. This Essay argues that the basic principles

---

[4] *See, e.g.*, Lawrence O. Gostin, *Health Information Privacy*, 80 CORNELL L. REV. 451, 512 (1995) ("The rule of confidentiality does not work nearly as well in a modern information society.").

[5] *See* Danielle Keats Citron, *Mainstreaming Privacy Torts*, 98 CAL. L. REV. 1805, 1836–50 (2010) (advocating judicial recognition of tortuous enablement, strict liability, and breach of confidence torts against website and database operators); Neil M. Richards & Daniel J. Solove, *Privacy's Other Path: Recovering the Law of Confidentiality*, 96 GEO. L.J. 123, 158 (2007) (noting that the American breach of confidentiality tort is less developed than the English one in that it "applies only to a limited set of relationships" and "third-party liability . . . has only been recognized in a few cases").

[6] *See* Patricia Sánchez Abril, *Private Ordering: A Contractual Approach to Online Interpersonal Privacy*, 45 WAKE FOREST L. REV. 689, 715–16 (2010) (highlighting that confidentiality agreements do not extend to third parties not in privity with the original parties).

[7] *Internet 2010 in Numbers*, PINGDOM (Jan. 12, 2011), http://royal.pingdom.com/2011/01/12/internet-2010-in-numbers/.

of confidentiality and contract law can create an attractive and broadly applicable remedy for protecting the personal information of Internet users. This remedy would allow the obligations of confidentiality to follow personal information downstream. Confidentiality doctrine could become more lenient by allowing for the limited disclosure of confidential information while also becoming more protective by having confidentiality obligations follow the information to third-party recipients. Courts and lawmakers could construct systems for confidentiality protections that follow the disclosed information in a chain-link fashion by requiring third-party recipients of confidential information to observe the same confidentiality obligations to which the initial recipient agreed.

Under a regime of chain-link confidentiality, Internet users could then pursue a remedy against anyone in the chain who either failed to abide by her obligation of confidentiality or failed to require confidentiality of a third-party recipient. Even if legislators decided not to create a private cause of action for Internet users, a statutory privacy bill of rights could breathe life into confidentiality doctrine by requiring obligations of confidentiality to follow the disclosure of personal information online.

This Essay explores various methods that courts and lawmakers can use to create a system of chain-link confidentiality in online data-sharing contexts. Part II of this Essay briefly explores the challenges and desirability of maintaining privacy in the digital age. This Part focuses on the failure of traditional remedies to protect online privacy, which necessitates a new approach that is clear, workable, and in harmony with other laws and policy goals, including the First Amendment's guarantee of freedom of speech. This part also responds to the critique that confidentiality law is of limited applicability. It explores the abundant opportunities for relationships and privity online and the concentration of disclosure of personal information to a surprisingly limited number of websites.

Part III introduces the general theory of chain-link confidentiality. A chain-link confidentiality approach would use contracts to link recipients of personal information. These

contracts would contain at least three kinds of terms: (1) obligations and restrictions on the use of the disclosed information; (2) requirements to bind future recipients to the same obligations and restrictions; and (3) requirements to perpetuate the contractual chain. The chief benefit of a chain-link confidentiality regime is that it would protect the downstream use of information in a clear and meaningful way. This Part explores the potential statutory and contractual applications of chain-link confidentiality.

This Essay concludes by highlighting how a chain-link confidentiality approach to protecting online privacy can be a flexible and effective compromise that protects the downstream use of information while accommodating the free flow of information.

II. PROTECTING PRIVACY IN THE DIGITAL AGE

The debate as to how to protect privacy can be frustrating because there is no fixed conceptualization of privacy.[8] Professor Daniel Solove called privacy "a concept in disarray" that encompasses, among other things, the "freedom of thought, control over one's body, solitude in one's home, control over personal information, freedom from surveillance, protection of one's reputation, and protection from searches and interrogations."[9]

---

[8] *See, e.g.*, DANIEL J. SOLOVE, UNDERSTANDING PRIVACY 1 (2008) [hereinafter SOLOVE, UNDERSTANDING PRIVACY] (noting that, despite the integral nature of privacy, nobody can articulate exactly what privacy means); *see also* JULIE C. INNESS, PRIVACY, INTIMACY, AND ISOLATION 3 (1992) (proposing to define and clarify privacy so as to construct an "escape route" from the confusion that underlies differing notions of privacy); ALAN F. WESTIN, PRIVACY AND FREEDOM 7 (1967) (observing that few fundamental rights remain as undefined as privacy); Ruth Gavison, *Privacy and the Limits of Law*, 89 YALE L.J. 421, 421–22 (1980) (discussing the confusion that exists between popular and legal concepts of privacy rights and the scholarly concept); Hyman Gross, *The Concept of Privacy*, 42 N.Y.U. L. REV. 34, 35 (1967) (stating that "the concept of privacy is infected with pernicious ambiguities"); Robert C. Post, *Three Concepts of Privacy*, 89 GEO. L.J. 2087, 2087 (2001) ("Privacy is a valve so complex, so entangled in competing and contradictory dimensions, so engorged with various and distinct meanings, that I sometimes despair whether it can be usefully addressed at all."); Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477, 477–78 (2006) [hereinafter Solove, *Taxonomy*] (proposing a new taxonomy of privacy to remedy the vagueness of the concept).

[9] SOLOVE, UNDERSTANDING PRIVACY, *supra* note 8, at 1.

The law's struggle to conceptualize privacy has often stunted its ability to adapt to rapid technological change.[10] That has been especially true with the Internet's rapid rise as courts grapple to define the contours of privacy in cyberspace.[11]

Given the abundance of personal information available on the Internet, privacy in the information age is a necessity.[12] Without it, Internet users are faced with the unappealing reality of complete transparency. The question of whether privacy is or should be protected by laws and policy seems more significant than ever. Congress introduced at least three privacy-related statutes at the federal level in 2011.[13] Congress has also held multiple hearings on the state of privacy.[14] The Federal Trade Commission (FTC) has made privacy one of its most important concerns.[15] The media have devoted substantial attention to the importance and erosion of privacy in the digital age.[16] A number

---

[10] *See, e.g.*, Richards, *supra* note 1, at 357 (arguing that the concept of tort privacy is ineffective in a digital age); Richards & Solove, *supra* note 1, at 1887 (explaining that Prosser's concept of privacy limits its adaptability in the Information Age); Solove, *supra* note 1, at 1089–90 (pointing out the need for an effective law of privacy in a world of constant technological change).

[11] *See, e.g.*, Moreno v. Hanford Sentinel, Inc., 91 Cal. Rptr. 3d 858, 863 (Cal. Ct. App. 2009) (holding that the plaintiff had no reasonable expectation of privacy for content posted on Myspace social network); *cf.* Pietrylo v. Hillstone Rest. Grp., No. 06-574 (FSH) 2008 WL 6085437, at *6–7 (D.N.J. July 25, 2008) (evaluating the expectation of privacy in an invitation-only Internet discussion space).

[12] *See infra* notes 19, 95–98 and accompanying text.

[13] Commercial Privacy Bill of Rights Act of 2011, S. 799, 112th Cong. (2011); Electronic Communications Privacy Act Amendments Act of 2011, S. 1011, 112th Cong. (2011); Do-Not-Track Online Act of 2011, S. 913, 112th Cong. (2011).

[14] *See, e.g.*, *The Electronic Communications Privacy Act: Government Perspectives on Protecting Privacy in the Digital Age: Hearing Before the S. Comm. on the Judiciary*, 112th Cong. (2011); Nicole Friess, *Senate Committee Holds Hearing on the State of Online Consumer Privacy*, INFO. L. GRP. (Mar. 16, 2011, 7:45 PM), http://www.infolawgroup.com/2011/03/articles/data-privacy-law-or-regulation/senate-committee-holds-hearing-on-the-state-of-online-consumer-privacy/ (discussing Senate Committee hearing on online consumer privacy); Brett Neely, *Sen. Franken Holds Washington Hearing on Smart Phone Privacy Issues*, MINNESOTA PUBLIC RADIO (May 10, 2011), http://minnesota.publicradio.org/display/web/2011/05/10/franken-hearing/ (discussing Judiciary Subcommittee hearing on smart phone privacy issues).

[15] *See* Kate Kaye, *Online Privacy: What to Expect in 2011*, CLICKZ (Jan. 3, 2011), http://www.clickz.com/clickz/news/1934456/online-privacy-expect-2011 (discussing the FTC's efforts regarding online privacy).

[16] *See, e.g.*, Steve Lohr, *How Privacy Can Vanish Online, a Bit at a Time*, N.Y. TIMES, Mar. 17, 2010, at A1 (discussing problems with the availability of personal information on

of high-profile issues, including body scanners at airports and commercial data breaches, have directly affected a significant portion of the American public.[17]

The greatest threat to an individual's privacy might be the collection, use, and dissemination of personal information on the Internet. These practices, which have been well-addressed by scholars,[18] leave Internet users vulnerable to a panoply of harms

---

the Internet); Jeffrey Rosen, *The End of Forgetting*, N.Y. TIMES, July 25, 2010, Magazine, at MM30 (discussing the problems of living in a world where the Internet records everything and forgets nothing).

[17] *See, e.g.*, Liana B. Baker & Jim Finkle, *Sony PlayStation Suffers Massive Data Breach*, REUTERS (Apr. 26, 2011, 7:36 PM), http://www.reuters.com/article/2011/04/26/us-sony-stoldendata-idUSTRE73P6WB20110426 (reporting breach in Sony's online game network that resulted in identity theft affecting millions of users); Jeremy Kirk, *Washington Post Reports Data Breach on Job Ads Section*, PCWORLD (July 7, 2011, 6:20 AM), http://www.pcworld.com/businesscenter/article/235189/washington_post_reports_data_breach_on_job_ads_section.html (reporting the Washington Post's alert regarding a data breach of its "Jobs" section); *Whole Body Imaging Technology and Body Scanners*, ELEC. PRIVACY INFO. CTR., http://epic.org/privacy/airtravel/backscatter/ (last visited Apr. 11, 2012) (arguing that body scanners are too invasive and discussing the effects of x-ray screening at transportation hubs).

[18] *See, e.g.*, DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE 2 (2004) [hereinafter SOLOVE, DIGITAL PERSON] (discussing "how we should understand and protect privacy in light of . . . profound technological developments"); Danielle Keats Citron & Frank Pasquale, *Network Accountability for the Domestic Intelligence Apparatus*, 62 HASTINGS L.J. 1441, 1441 (2001) (arguing that "[a] new concept of accountability—'network accountability'—is needed to address the shortcomings of fusion centers," which are governmental sites that collect and share information); A. Michael Froomkin, *The Death of Privacy?*, 52 STAN. L. REV. 1461, 1463 (2000) (discussing new technologies that allow for easier and cheaper data collection and arguing that, "when possible, the law should facilitate informational privacy"); Chris Jay Hoofnagle, *Big Brother's Little Helpers: How ChoicePoint and Other Commercial Data Brokers Collect and Package Your Data for Law Enforcement*, 29 N.C. J. INT'L L. & COM. REG. 595, 595 (2004) ("Lawmakers should revisit federal privacy laws to account for private-sector database companies that sell personal information to the government for law enforcement purposes."); Sarah Ludington, *Reining in the Data Traders: A Tort for the Misuse of Personal Information*, 66 MD. L. REV. 140, 140 (2006) (arguing that "a new common law tort should be used to force reform and accountability on data traders, and to provide remedies for individuals who have suffered harm to their core privacy interests of choice and control"); Helen Nissenbaum, *Privacy as Contextual Integrity*, 79 WASH. L. REV. 119, 119 (2004) (arguing for a theory of "contextual integrity," which would "tie[ ] adequate protection for privacy to norms of specific contexts, demanding that information gathering and dissemination be appropriate to that context and obey the governing norms of distribution within it"); Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701, 1701 (2010) (discussing possible ways to remedy the problem that "scientists . . . can often 'reidentify' or 'deanonymize' individuals hidden in anonymized data with astonishing ease"); Neil M. Richards, *Intellectual Privacy*, 87 TEX. L. REV. 387, 387 (2008) (discussing "the protection of

including excessive government and commercial entity surveillance, breach of confidentiality, misuse of personal information for such things as denial of employment or insurance benefits, damage to reputation, blackmail, loss of anonymity, chilled speech or association, and extreme emotional distress.[19]

Thankfully, privacy has been valued by many courts and lawmakers. Notwithstanding the difficulty in defining privacy, it has been recognized, to varying degrees, as a civil right both in the United States and in other nations. The European Union explicitly views privacy as a human right.[20] The European Union

---

records of our intellectual activities—and how legal protection of these records is essential to the First Amendment values of free thought and expression"); Neil M. Richards, *The Information Privacy Law Project*, 94 GEO. L.J. 1087, 1087 (2006) [hereinafter Richards, *Information Privacy*] (discussing and assessing "the emergence of 'The Information Privacy Law Project,' a group of scholars focused on the legal issues raised by the increasing collection, use, and disclosure of personal information made possible by evolving digital technologies"); Paul M. Schwartz & Edward J. Janger, *Notification of Data Security Breaches*, 105 MICH. L. REV. 913, 913 (2007) (arguing that current requirements that companies disclose security breaches involving personal information are insufficient and proposing more effective notification processes for such breaches); Paul M. Schwartz, *Property, Privacy, and Personal Data*, 117 HARV. L. REV. 2055, 2055 (2004) (developing "a model of propertized personal information that responds to . . . serious concerns about privacy"); Daniel J. Solove, *Data Mining and the Security-Liberty Debate*, 75 U. CHI. L. REV. 343, 345 (2008) (arguing that "data mining's security benefits require more scrutiny, and [that] the privacy concerns are significantly greater than currently acknowledged").

[19] *See, e.g.*, M. Ryan Calo, *The Boundaries of Privacy Harm*, 86 IND. L.J. 1131, 1131 (2011) (describing privacy violations as falling into "objective" and "subjective" categories); Solove, *Taxonomy*, *supra* note 8, at 478 (arguing for "[a] new taxonomy to understand privacy violations").

[20] *See, e.g.*, Convention for the Protection of Human Rights and Fundamental Freedoms, art. 8(1), Nov. 4, 1950, 213 U.N.T.S. 221 ("Everyone has the right to respect for his private and family life, his home and his correspondence."); Council Directive 95/46/EC, art. 1(1), 1995 O.J. (L 281) 31, 38 (stating that people have a "right to privacy with respect to the processing of personal data"); *see also* PETER P. SWIRE & ROBERT E. LITAN, NONE OF YOUR BUSINESS: WORLD DATA FLOWS, ELECTRONIC COMMERCE, AND THE EUROPEAN PRIVACY DIRECTIVE, at vii (1998) (discussing the European Union Directive "designed to improve privacy protection in its member countries"); Fred H. Cate, *European Court of Human Rights Expands Privacy Protections:* Copeland v. United Kingdom, 11 AM. SOC'Y INT'L L. INSIGHT (Aug. 6, 2007), *available at* http://www.asil.org/insights070806.cfm (discussing recent case in which protections of personal information were extended); Joel R. Reidenberg, *E-Commerce and Trans-Atlantic Privacy*, 38 HOUS. L. REV. 717, 731 (2001) ("Europe treats privacy as a political imperative anchored in fundamental human rights."); Spiros Simitis, *From the Market to the Polis: The EU Directive on the Protection of Personal Data*, 80 IOWA L. REV. 445, 448 (1995) (noting that "democratic society cannot and will not function without rules governing the processing of personal data"). *See generally* Symposium, *Data Protection Law and the European Union's Directive: The Challenge for the*

Data Protection Directive of 1995 imposes a number of obligations on the processors of personal data, including the requirement that processors obtain unambiguous consent from the individual for the transfer of certain data.[21] The directive gives individuals the right to exert some control over the use of data about them, the right to be notified about personal information collection, the right to correct inaccurate information, the right to object to the use or transfer of information, and the right not to be subject to certain automated decisions.[22]

In the United States, certain aspects of privacy have been explicitly protected, such as the right to be free from unreasonable government search and seizure[23] and the right to anonymity.[24] Numerous statutes have been enacted to preserve an individual's privacy.[25] The common law provides multiple actions in tort to

---

United States, 80 IOWA L. REV. 431 (1995) (discussing the EU Data Protection Directive and its impact on the United States).

[21] Council Directive 95/46/EC, art. 7(a), 1995 O.J. (L 281) 31, 40.

[22] Council Directive 95/46/EC, arts. 7, 10, 12, 14–15, 1995 O.J. (L 281) 31, 40–43.

[23] U.S. CONST. amend. IV.

[24] *See, e.g.*, Katz v. United States, 389 U.S. 347, 350 (1967) (stating that the Fourth Amendment "protects individual privacy against certain kinds of government intrusion"); NAACP v. Alabama *ex rel.* Patterson, 357 U.S. 449, 462 (1958) ("Inviolability of privacy in group association may in many circumstances be indispensable to preservation of freedom of association, particularly where a group espouses dissident beliefs."); *cf.* Reidenberg, *supra* note 20, at 730–31 ("While there is a consensus among democratic states that information privacy is a critical element of civil society, the United States has, in recent years, left the protection of privacy to markets rather than law.").

[25] *See, e.g.*, Right to Financial Privacy Act (RFPA) of 1978, 12 U.S.C. §§ 3401–3422 (2006) (protecting the confidentiality of consumers' financial information from the government); Fair Credit Reporting Act (FCRA), 15 U.S.C. § 1681(a)(4) (2006) (noting "[t]here is a need to insure that consumer reporting agencies exercise their grave responsibilities with . . . respect for the consumer's right to privacy"); Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501–6506 (2006) (requiring parental consent for a website to gather personal information about a child under the age of thirteen); Video Voyeurism Prevention Act of 2004, 18 U.S.C. § 1801 (2006) (criminalizing the capturing of an image of a private area of an individual without their consent when the individual has reasonable expectation of privacy); Electronic Communications Privacy Act (ECPA) of 1986, 18 U.S.C. §§ 2510–2522 (2006) (guarding privacy rights from infringement by wire or electronic communication intercepting devices); Video Privacy Protection Act of 1988, 18 U.S.C. §§ 2701–2712 (2006) (criminalizing obtaining, altering, or preventing authorized access to a wire or electronic communication in electronic storage via unauthorized access to a facility through which an electronic communication service is provided); Driver's Privacy Protection Act of 1994, 18 U.S.C. §§ 2721–2725 (2006) (criminalizing certain unauthorized uses of personal information obtained from a motor vehicle record); Foreign Intelligence Surveillance Act (FISA) of 1978, 50 U.S.C. §§ 1801–1811 (2006) (regulating the gathering of

vindicate one's privacy rights.[26] Social science has long supported the fundamental and intrinsic need for privacy in our everyday lives, most recently on the Internet.[27] In short, the protection of our privacy in the digital age is essential.[28]

The challenge with privacy protection in the law, particularly with respect to the Internet, is implementation.[29] Internet privacy laws that are defined too narrowly fail to address the complete array of privacy problems. Yet if Internet privacy laws are too broad, they become either meaningless or too difficult to enforce effectively. The result is that a single approach likely is inadequate to address the full range of current privacy problems.[30]

---

electronic surveillance of foreign entities); Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (codified as amended at 42 U.S.C. §§ 201–300ii (2006)) (regulating the use of information gathered from health insurance information); Fair and Accurate Credit Transactions Act (FACTA) of 2003, Pub. L. No. 108-159, 117 Stat. 1952 (codified as amended at 15 U.S.C. § 1681 (2006)) (protecting consumers against inaccurate and unfair credit billing and credit card practices).

[26] *See, e.g.*, RESTATEMENT (SECOND) OF TORTS §§ 652B–652E (1977) (describing the torts of intrusion upon seclusion, appropriation of name or likeness, public disclosure of private facts, and public placing person in false light).

[27] *See generally* IRWIN ALTMAN, THE ENVIRONMENT AND SOCIAL BEHAVIOR (1975) (analyzing the interaction between privacy, crowding, territory, and personal space); ERVING GOFFMAN, BEHAVIOR IN PUBLIC PLACES: NOTES ON THE SOCIAL ORGANIZATION OF GATHERINGS (1963) (discussing how people form perceptions of others through outward manifestations of personal characteristics); ERVING GOFFMAN, THE PRESENTATION OF SELF IN EVERYDAY LIFE (1959) (same); SANDRA PETRONIO, BOUNDARIES OF PRIVACY: DIALECTICS OF DISCLOSURE (2002) (analyzing individual privacy in a context of disclosure and nondisclosure of private information); WESTIN, *supra* note 8 (discussing methods for protecting privacy in an age where technology makes gathering private information increasingly easy); danah boyd, *Why Youth (Heart) Social Network Sites: The Role of Networked Publics in Teenage Social Life*, *in* YOUTH, IDENTITY, AND DIGITAL MEDIA 119, 131–32 (David Buckingham ed., 2008) (discussing how teenagers manage the privacy of their public images on social networking sites).

[28] *See, e.g.*, SOLOVE, DIGITAL PERSON, *supra* note 18, at 2 (exploring how old conceptions of privacy are not suited for understanding and protecting privacy in an Information Age); Daniel J. Solove, *The Virtues of Knowing Less: Justifying Privacy Protections Against Disclosure*, 53 DUKE L.J. 967, 970 (2003) ("Given the development of technologies that permit extensive data gathering and dissemination, deciding how to regulate the disclosure of personal information is a vital issue.").

[29] *See generally* Kenneth A. Bamberger & Deirdre K. Mulligan, *Privacy on the Books and on the Ground*, 63 STAN. L. REV. 247 (2011) (providing a descriptive account of the implementation of privacy management and arguing for improvement in privacy regulations).

[30] *See, e.g.*, Froomkin, *supra* note 18, at 1466 (noting that, while no single solution may exist, a combination of legal approaches may alleviate some of the concerns in Internet privacy law).

If privacy is to be effectively protected by the law, it must be done through a combination of statutory law, common law, equity, and administrative doctrines. While our current privacy protection regime is a patchwork of laws and remedies, the regime is often muddled or in conflict with other laws and evolving technology.[31] Many of the current privacy protections focus on the nature or use of personal information. For example, several privacy remedies, such as the public disclosure of private facts and false light torts, only restrict information that is "highly offensive to a reasonable person."[32] Privacy laws limiting the collection or disclosure of certain kinds of information or laws that are based on particular kinds of technology seem to create the most confusion.[33]

These approaches have merit, but it is dangerous for privacy laws to place too much reliance on the inconsistently applied standard of "private" information or subjective tests like "reasonable expectations of privacy."[34] Approaches that focus on the nature of the information are problematic because personal information is usually not seen as strictly private or public.[35] The

---

[31] *See* James T. O'Reilly, *Homeland Security and the Future of Privacy Rights: A Commentary*, 55 FED. LAW. 54, 54 (June 2008) (attributing the conflicting body of laws to a lack of sustained public interest in privacy).

[32] RESTATEMENT (SECOND) OF TORTS §§ 652D, 652E (1977).

[33] *See, e.g.*, Electronic Communications Privacy Act (ECPA) of 1986, 18 U.S.C. §§ 2510–2522 (2006) (classifying all regulated communication into three types: "wire communication," "oral communication," and "electronic communication"); Deirdre K. Mulligan, *Reasonable Expectations in Electronic Communications: A Critical Perspective on the Electronic Communications Privacy Act*, 72 GEO. WASH. L. REV. 1557, 1571–72 (2004) (pointing out that the complicated body of electronic privacy law is confusing both for laypersons and for lawyers). *See generally* Symposium, *The Future of Internet Surveillance Law: A Symposium to Discuss Internet Surveillance, Privacy & the USA Patriot Act*, 72 GEO. WASH. L. REV. 1139 (2004) (discussing internet surveillance, privacy, and the USA Patriot Act to help define the field of Internet surveillance law); *ECPA Reform: Why Now?*, DIGITAL DUE PROCESS, http://www.digitalddueprocess.org/index.cfm?objectid=37940370-2551-11DF-8E02000C296BA163 (last visited Apr. 11, 2012) ("[ECPA] has not undergone a significant revision since it was enacted in 1986—light years ago in Internet time. As a result, ECPA is a patchwork of confusing standards that have been interpreted inconsistently by the courts, creating uncertainty for both service providers and law enforcement agencies.").

[34] *See, e.g.*, Daniel J. Solove, *Fourth Amendment Pragmatism*, 51 B.C. L. REV. 1511, 1511 (2010) (arguing that the "reasonable expectation of privacy test should be abandoned").

[35] *See, e.g.*, HELEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE 90 (2010) (scrutinizing the different meanings of public and private depending upon the arena of discussion); Nissenbaum, *supra* note 18, at 132 (explaining that "[i]nterpretations of what counts as a private space may vary across times,

same piece of information can be considered sensitive in some circumstances and completely benign in others. Approaches that focus on the use of information are better because the use of information is what often leads to privacy harms.[36] Additionally, any law aimed at the suppression of a particular kind of expression is suspect under the First Amendment.[37] Thus, any scheme for protecting privacy in an online environment should be manageable, effective, clearly defined, and constitutionally valid. The concept of chain-link confidentiality could meet all of these demands.

A. THE PROMISE IN EVOLVING CONFIDENTIALITY

The subtext behind the recent proposals to protect privacy is that the traditional privacy remedies are inadequate in the digital age. The aggregated, searchable, and semi-permanent nature of online information has allowed anyone with access to the Internet the power of unlimited distribution and perfect recall. This titanic shift in the way we disclose and receive information on the Internet has magnified an individual's potential privacy harms.[38] The idea of Prosser's four privacy torts serving as the chief legal mechanisms to protect online privacy almost seems quaint.[39]

---

societies, and cultures"); Sharon K. Sandeen, *Relative Privacy: What Privacy Advocates Can Learn from Trade Secret Law*, 2006 MICH. ST. L. REV. 667, 692–94 (evaluating the historical conflation of privacy and secrecy); Lior Jacob Strahilevitz, *A Social Networks Theory of Privacy*, 72 U. CHI. L. REV. 919, 919 (2005) (arguing for an empirical approach in determining whether certain information should be considered private or public).

[36] *See* Calo, *supra* note 19, at 1133 (arguing that one of two categories of privacy harm "is the unanticipated or coerced use of information concerning a person against that person").

[37] *See* Solveig Singleton, *Privacy Versus the First Amendment: A Skeptical Approach*, 11 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 97, 112–14 (2000) (finding that "miscellaneous" privacy torts, such as the tort of disclosure of embarrassing facts, frequently run into First Amendment issues); Eugene Volokh, *Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People from Speaking About You*, 52 STAN. L. REV. 1049, 1122 (2000) (arguing that all restrictions on speech, even against highly embarrassing or valueless speech, raise strong doctrinal problems); Diane L. Zimmerman, *Requiem for a Heavyweight: A Farewell to Warren and Brandeis's Privacy Tort*, 68 CORNELL L. REV. 291, 311–20 (1983) (describing the Court's great skepticism towards forbidding truthful or improperly motivated speech).

[38] *See* Citron, *supra* note 2, at 69–70 (observing that twenty-first century technologies have intensified mental and reputational injuries, multiplied financial injuries, and exacerbated physical injuries).

[39] *See id.* at 89 (arguing that traditional tort law is not a sufficient response to online

Professor Susan Gilles observed that the privacy torts have "had a far from happy life."[40] The torts, as well as a number of statutes designed to protect privacy, are too vague, too subjective, or too technology-dependent and, thus, outdated. Privacy scholars have suggested modifying the privacy torts,[41] passing new legislation, altering existing statutes,[42] or simply giving up on the concept of privacy and embracing our new transparent society.[43]

One of the most promising alternatives to the oft-maligned privacy torts that scholars have proposed is the law of confidentiality.[44] Professors Neil Richards and Daniel Solove

---

abuse and that civil rights laws should be enforced in that context); Richards, *supra* note 1, at 357 (arguing that as "interpreted by [ ] Prosser, tort privacy is a poor vehicle for grappling with problems of privacy and reputation in the digital age"); Singleton, *supra* note 37, at 118–19 (describing multiple bills pending in Congress to regulate Internet privacy); Zimmerman, *supra* note 37, at 362 (recognizing that common law private-facts torts do not effectively address new privacy questions arising from the exchange of computerized information).

[40] Susan M. Gilles, *Promises Betrayed: Breach of Confidence as a Remedy for Invasions of Privacy*, 43 BUFF. L. REV. 1, 7 (1995).

[41] *See, e.g.*, Patricia Sánchez Abril, *Recasting Privacy Torts in a Spaceless World*, 21 HARV. J.L. & TECH. 1, 6 (2007) ("By reconceptualizing the tort without reference to space, this Article aims to articulate and support a practicable, factor-driven approach to the public disclosure tort . . . ."); Ludington, *supra* note 18, at 140 (arguing "that the existing scheme of common law privacy torts should be expanded to create a new tort for information misuse"); Joseph Elford, Note, *Trafficking in Stolen Information: A "Hierarchy of Rights" Approach to the Private Facts Tort*, 105 YALE L.J. 727, 729 (1995) (advocating a method-focused approach to the private-facts tort).

[42] *See, e.g.*, Jacqueline D. Lipton, *"We, the Paparazzi": Developing a Privacy Paradigm for Digital Video*, 95 IOWA L. REV. 919, 954 (2010) ("[L]egal rules could improve online-privacy regulation by recognizing reasonable expectations of privacy even in public spaces traditionally unprotected by privacy torts; better protecting confidential relationships; and allowing 'individuals to exercise greater control over their personal information, . . . after it has been exposed' to other people or even to the general public." (quoting DANIEL SOLOVE, THE FUTURE OF REPUTATION: GOSSIP, RUMOR, AND PRIVACY ON THE INTERNET 188 (2007)) (internal footnotes omitted)).

[43] *See, e.g.*, DAVID BRIN, THE TRANSPARENT SOCIETY: WILL TECHNOLOGY FORCE US TO CHOOSE BETWEEN PRIVACY AND FREEDOM? 3–5 (1998) (advocating an embrace of inevitable transparency as a way to empower citizens).

[44] *See, e.g.*, Randall P. Bezanson, *The Right to Privacy Revisited: Privacy, News, and Social Change, 1890–1990*, 80 CALIF. L. REV. 1133, 1133–34 (1992) ("[T]he legal emphasis on controls over publication [should] be shifted to a duty of confidentiality imposed on those possessing private information."); Gilles, *supra* note 40, at 14–15 ("American law is in the process of recognizing three distinct theories—contract, fiduciary duty and perhaps tort—which can be used to found an action against a confidant who reveals information."); Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193, 1193–94 (1998) (arguing for a default rule that allows for only the "functionally necessary"

argued in an influential article embracing confidentiality law that "Warren and Brandeis rejected confidentiality as too restrictive and narrow a basis for protecting privacy, but they did not envision just how flexibly the concept could be used."[45] Gilles noted that, given the bleak future of the privacy torts, "some have advocated that American courts take a second look at breach of confidence and assess its ability to protect privacy."[46]

Compared to the concept of privacy, confidentiality is relatively straightforward. *Black's Law Dictionary* defines confidentiality as

---

processing of personal information unless the parties expressly agree otherwise); Andrew J. McClurg, *Kiss and Tell: Protecting Intimate Relationship Privacy Through Implied Contracts of Confidentiality*, 74 U. CIN. L. REV. 887, 888 (2006) (proposing that an implied contract of confidentiality arises in intimate relationships that the parties will not disseminate private information through mass communication); Pamela Samuelson, *Privacy as Intellectual Property?*, 52 STAN. L. REV. 1125, 1125 (2000) (urging the adoption of certain trade secrecy laws to protect personal information online); Sandeen, *supra* note 35, at 697 (advocating for the application of the relative secrecy doctrine to the protection of personal information); Jay Weiser, *Measure of Damages for Violation of Property Rules: Breach of Confidentiality*, 9 U. CHI. L. SCH. ROUNDTABLE 75, 76 (2002) (explaining that property rules should be used to protect confidentiality); Peter A. Winn, *Confidentiality in Cyberspace: The HIPAA Privacy Rules and the Common Law*, 33 RUTGERS L.J. 617, 619 (2002) (arguing that breach of confidentiality can provide an effective remedy for the improper disclosure of health information); Steven A. Bibas, Note, *A Contractual Approach to Data Privacy*, 17 HARV. J.L. & PUB. POL'Y 591, 605–06 (1994) (advocating a contractual solution to data and privacy problems); Scott L. Fast, Comment, *Breach of Employee Confidentiality: Moving Toward a Common-Law Tort Remedy*, 142 U. PA. L. REV. 431, 433 (1993) (arguing that courts should provide a common law remedy for disclosures to third parties in the employer–employee context); G. Michael Harvey, Comment, *Confidentiality: A Measured Response to the Failure of Privacy*, 140 U. PA. L. REV. 2385, 2392 (1992) (advocating for a legally enforceable duty of confidentiality that attaches when a person engages in an unauthorized publication of information); Alan B. Vickery, Note, *Breach of Confidence: An Emerging Tort*, 82 COLUM. L. REV. 1426, 1426 (1982) (concluding that the basis for imposing liability for breach of confidence should be the disclosure of information revealed in the course of a nonpersonal relationship of a sort customarily understood to carry an obligation of confidentiality).

[45] Richards & Solove, *supra* note 5, at 173; *see also* Daniel J. Solove & Neil M. Richards, *Rethinking Free Speech and Civil Liability*, 109 COLUM. L. REV. 1650, 1669 (2009) ("[T]he realist critique of the distinctions between tort, contract, and property suggests that the formalist approach is not as clear-cut as it might at first seem.").

[46] Gilles, *supra* note 40, at 9 (footnote omitted); *see also* Bezanson, *supra* note 44, at 1174 ("I suggest that the privacy tort be formally interred, and that we look to the concept of breach of confidence to provide legally enforceable protection from dissemination of identified types of personal information."); Zimmerman, *supra* note 37, at 363 ("More thought should also be given to increasing the use of legal sanctions for the violation of special confidential relationships, in order to give individuals greater control over the dissemination of personal information." (footnote omitted)).

"the state of having the dissemination of certain information restricted."[47] Ethicist Sissela Bok defined confidentiality as "the boundaries surrounding shared secrets and . . . the process of guarding these boundaries. While confidentiality protects much that is not in fact secret, personal secrets lie at its core."[48] The law will impose an obligation of confidentiality on recipients of information when they have agreed not to share the information with third parties or when they receive information within the context of a confidential relationship.[49] Obligations or privileges of confidentiality are found in multiple areas of the law in the United States, including express and implied contracts for confidentiality,[50] the still-developing tort of breach of confidence,[51] evidentiary privileges regarding confidentiality,[52] procedural protections like protective orders to prevent the disclosure of embarrassing personal information in court records,[53] and statutes explicitly creating confidential relationships.[54]

---

[47] BLACK'S LAW DICTIONARY 339 (9th ed. 2009).

[48] SISSELA BOK, SECRETS: ON THE ETHICS OF CONCEALMENT AND REVELATION 119 (1982).

[49] Solove & Richards, *supra* note 45, at 1669 ("There are also other confidentiality rules not involving civil liability, such as criminal prohibitions on divulging certain kinds of confidential information, evidentiary privileges restricting testimony about confidential data, and statutory protections that limit the release of confidential information by certain companies or government agencies." (footnote omitted)).

[50] *See, e.g.*, McClurg, *supra* note 44, at 908–11 (advocating the adoption of contract remedies for breach of implied or express confidentiality agreements).

[51] *See, e.g.*, Vickery, *supra* note 44, at 1448–52 (examining the scope of the emerging tort of breach of confidence).

[52] *See, e.g.*, Richards & Solove, *supra* note 5, at 134–35 (discussing the recognition of evidentiary privileges for confidential information in U.S. case law).

[53] *See, e.g.*, FED. R. CIV. P. 26(c)(1) (authorizing protective orders "to protect a party or person from annoyance, embarrassment, [or] oppression"); *see also* Freedom of Information Act (FOIA), 5 U.S.C. § 552(b)(6) (2006) (providing an exemption from the disclosure of personnel and medical files if the disclosure "would constitute a clearly unwarranted invasion of personal privacy").

[54] *See, e.g.*, Fair Credit Reporting Act (FCRA), 15 U.S.C. §§ 1681–1681x (2006) (regulating the collection, dissemination, and use of consumer information); Financial Services Modernization (Gramm–Leach–Bliley) Act of 1999, 15 U.S.C. §§ 6801–6809 (2006) (requiring financial institutions to provide each customer with a notification about their privacy rights at the time the consumer is established and annually thereafter); Video Privacy Protection Act of 1988, 18 U.S.C. § 2710(b)(2)(B) (2006) (preventing the disclosure of rental records of videos or other audiovisual materials); Health Insurance Portability and Accountability Act (HIPAA) of 1996, 42 U.S.C. §§ 1320d–1320d-8 (2006) (regulating the disclosure of information related to an individual's health care).

Typically, obligations of confidentiality arise through voluntary promises or agreements to respect designated information. They are also created through consensual confidential relationships.[55] Confidentiality agreements are legally binding agreements that are commonly used to prohibit the disclosure of information. [56] Such contracts are used to protect anonymity, arbitration proceedings,[57] settlement agreements,[58] and trade secrets.[59] Additionally, these contracts may protect sensitive information such as health information, sexual preferences, intimate feelings, and other pieces of similarly personal information.[60] Even quasi-contractual promises of confidentiality are enforceable if disclosers of information rely on them to their detriment.[61]

In addition to confidentiality agreements, an obligation of confidentiality may be created by entering into a confidential or fiduciary relationship. The law of equity has traditionally designated certain relations, such as principal–agent and trustee–beneficiary, as "fiduciary."[62] Gilles wrote that "[w]here such a relation exists, a fiduciary is under a duty 'to act for the benefit of

---

[55] Gilles, *supra* note 40, at 15.

[56] *See id.* ("Express written contracts, binding the signer to hold information confidential, have long been used in the commercial area, particularly by employers to prevent employees from revealing business secrets.").

[57] *See, e.g.*, Amy J. Schmitz, *Untangling the Privacy Paradox in Arbitration*, 54 U. KAN. L. REV. 1211, 1212 (2006) (describing the value of confidentiality agreements in arbitration proceedings).

[58] *See, e.g.*, Laurie Kratky Doré, *Secrecy by Consent: The Use and Limits of Confidentiality in the Pursuit of Settlement*, 74 NOTRE DAME L. REV. 283, 286 (1999) (noting that courts permit confidentiality agreements to encourage parties to settle).

[59] *See, e.g.*, Samuelson, *supra* note 44, at 1152 (explaining how a confidentiality agreement to protect trade secrets typically works).

[60] *See, e.g.*, Hammonds v. Aetna Cas. & Sur. Co., 243 F. Supp. 793, 801 (N.D. Ohio 1965) (holding that a contract between a doctor and a patient contains an implied condition for the doctor not to release any confidential information gained through the contractual relationship without the patient's permission); Richards & Solove, *supra* note 5, at 136–38 (discussing early cases where courts created a legal remedy for divulging confidential information based on implied contract).

[61] *See, e.g.*, Cohen v. Cowles Media Co., 479 N.W.2d 387, 391 (Minn. 1992) (applying promissory estoppel where newspapers breached promises of confidentiality), *on remand from* 501 U.S. 663 (1991). Promissory estoppel is an equitable doctrine designed to enforce promises that are detrimentally relied upon even though the formal elements of a contract are not present. Woodrow Hartzog, *Promises and Privacy: Promissory Estoppel and Confidential Disclosure in Online Communities*, 82 TEMP. L. REV. 891, 909 (2009).

[62] Gilles, *supra* note 40, at 39.

the other party to the relation as to matters within the scope of the relation.' This duty, often characterized as the 'duty of loyalty,' includes an obligation not to reveal information."[63]

Like confidentiality agreements, the existence of a confidential relationship is a question of fact.[64] Professor Roy Ryden Anderson found that "confidential relationships have been labeled 'fact-based' fiduciary relationships to distinguish them from formal [fiduciary relationships]."[65] Although professional relationships such as doctor–patient and attorney–client relationships are the most common types of confidential relationships, courts have found many kinds of relationships to be confidential, including friendships, business relationships, and familial relationships.[66]

Breach of these confidential relationships can, in some instances, give rise to liability under the breach of confidence tort. This tort, while well-developed in England, is limited in the United States.[67] The tort is deceptively simple, as "[c]ourts impose liability under the tort when a person discloses information that he received in confidence."[68] While the tort has been most successful with regard to professional relationships, liability can

---

[63] *Id.* at 39–40 (quoting AUSTIN W. SCOTT & WILLIAM F. FRATCHER, THE LAW OF TRUSTS § 2.5 (4th ed. 1987) (footnote omitted)).

[64] Roy Ryden Anderson, *The Wolf at the Campfire: Understanding Confidential Relationships*, 53 SMU L. REV. 315, 317 (2000).

[65] *Id.* (footnote omitted).

[66] *See id.* at 330 (noting the categories courts use in determining the existence of a confidential relationship); *see also* GEORGE G. BOGERT, THE LAW OF TRUSTS AND TORTS § 482, at 284–86 (2d ed. 1981) ("Equity has never bound itself by any hard and fast definition of the phrase 'confidential relation' and has not listed all the necessary elements of such a relation, but has reserved discretion to apply the doctrine whenever it believes that a suitable occasion has arisen."). Gilles identified some factors that courts consider in determining whether a confidential relation exits: "the length of time of the reliance, a disparity in the positions of the parties, and a close relationship between the parties. It is 'great intimacy, disclosure of secrets, entrusting of power, and superiority of position' that evidence a confidential relation." *Id.* (quoting BOGERT, *supra,* § 482, at 281, 287–319).

[67] *See* Gilles, *supra* note 40, at 4–14 (tracing the English breach of confidence tort and the American invasion of privacy tort to their common doctrinal ancestor); Harvey, *supra* note 44, at 2392–93 (noting the breach of confidence doctrine in England and stating American courts' basis for rejecting it); Richards & Solove, *supra* note 5, at 156–58, 180 (discussing how American courts have largely ignored the breach of confidentiality tort). *See generally* PAUL STANLEY, THE LAW OF CONFIDENTIALITY: A RESTATEMENT (2008) (stating the fundamental principles underlying the modern English law of confidentiality).

[68] Alan E. Garfield, *Promises of Silence: Contract Law and Freedom of Speech*, 83 CORNELL L. REV. 261, 341 (1998).

also occur "in an informal setting if the party receiving the information either explicitly or implicitly agrees to keep the information confidential."[69]

From a doctrinal perspective, the law of confidentiality offers many benefits over the common law privacy torts and current privacy statutes. Under the law of confidentiality, courts can largely avoid the difficult question of whether information was private, newsworthy, or offensive, and focus instead on whether a trust was breached.[70] Information can typically be protected by a duty of confidentiality without regard to the extent that it has been disclosed to others.[71] Additionally, the law of confidentiality is less constitutionally suspect than the disclosure tort, which has significant First Amendment limitations.[72] The Supreme Court

---

[69] *Id.* (footnote omitted).

[70] *See, e.g.*, Richards & Solove, *supra* note 5, at 178 (noting that confidentiality law focuses on the source, rather than the content, of information); Winn, *supra* note 44, at 653–54 ("Claims for invasion of privacy . . . are based on the misuse of the personal information due to the sensitive and private nature of the information. On the other hand, breach of confidentiality represents an injury to a relationship of trust between the injured person and the person who has misused the information . . . .").

[71] *See, e.g.*, Winn, *supra* note 44, at 657 ("[I]n the tort of breach of confidentiality, the unauthorized revelation of confidential medical information is protected without regard to the degree to which the information has been published to the general public."). It is important to note that some conceptions of confidentiality will not protect information that is publicly available. *See* Abril, *supra* note 6, at 713 ("Fundamentally, a confidentiality agreement cannot shield information that is publicly available." (footnote omitted)); *cf.* Smith v. Dravo Corp., 203 F.2d 369, 375 (7th Cir. 1953) (holding that an obligation of confidentiality can still exist even if information is publicly available if the discloser somehow saved the recipient time and effort in disclosing the information or presented the information in a more ready and usable form than what was publicly available). The interpretation of "publicly available" also varies wildly, particularly online, and is outside the scope of this Essay. *See* Woodrow Hartzog & Frederic D. Stutzman, *The Case for Online Obscurity*, 101 CALIF. L. REV. (forthcoming 2013) (manuscript at 17–31) (arguing that the public/private dichotomy provides an inadequate account of online privacy), *available at* http://ssrn.com/abstract=1597745.

[72] *See, e.g.*, Paul M. Schwartz, Comment, *Free Speech vs. Information Privacy: Eugene Volokh's First Amendment Jurisprudence*, 52 STAN. L. REV. 1559, 1561–63 (2000) (arguing that fair information practices are a narrow exception to First Amendment limitations); Singleton, *supra* note 37, at 98–114 (providing a historical overview of tensions between privacy law and the First Amendment in the United States); Volokh, *supra* note 37, at 1122–23 (concluding that much of American privacy law presents unavoidable First Amendment problems); Winn, *supra* note 44, at 658 ("There is no defense to an action for breach of confidentiality that facts disclosed are of public interest."); Zimmerman, *supra* note 37, at 294 (stating that many justifications of the Warren–Brandeis right of privacy "have often underplayed its serious constitutional problems").

ruled in *Cohen v. Cowles Media Co.*[73] that the First Amendment does not bar an action for breach of a promise of confidentiality.[74]

Yet, confidentiality law also has flaws that might not make it a good fit to protect online privacy. As discussed below, confidentiality law provides a remedy only against the initial recipient of information. It does not provide a remedy against third parties who are exposed to and use information downstream. Unless an action is brought using the breach of confidence tort, damages can only be collected under more limited recovery regimes, such as contract law.[75]

Obligations imposed by confidentiality law may also be too burdensome in realms where the free flow of information is lauded, encouraged, and, in many contexts, necessary. The traditional hallmark of confidentiality law is its role in locking down information. The obligations of those bound to confidentiality are often simple and strict: do not disclose the information received in confidence. While confidentiality works remarkably well in many instances, it might over-protect information if it were to be widely adopted online and unduly inhibit the flow of information. Chain-link confidentiality can alleviate the friction here between lockdown and unrestrained publicity. No environment for disclosure could benefit from this compromise more than the Internet.

B. THE POTENTIAL FOR PRIVITY ONLINE

In suggesting confidentiality law as a potential alternative to Prosser's privacy torts, Professor Danielle Keats Citron also noted that a confidentiality approach has important limits. Citron observed that "[b]ecause it requires the existence of a relationship to which it is reasonable to impose duties of confidence, it would likely not apply to data brokers and others who lack a relationship

---

[73] 501 U.S. 663 (1991).

[74] *Id.* at 670.

[75] *See, e.g.*, Gilles, *supra* note 40, at 3 (noting that the "formal requirements and inadequate damages" of contract remedies render them less attractive than a breach of confidence tort).

with individuals whose information they release."[76] Richards and Solove also noted the limitations of confidentiality law:

> As Warren and Brandeis themselves recognized over a century ago, breach of confidence is a poor cause of action to assert against strangers who take and publish nonconsensual photographs of people. An action for breach of confidence protects information given by the confider to the confidant, but not information communicated outside that relationship. Thus, a third party can freely disclose private facts about a person as long as the third party did not learn the information from a confidant.[77]

In this important respect, confidentiality law as traditionally conceived is of limited effectiveness. But, the effectiveness of confidentiality law need not be limited online. This Essay posits that the Internet is capable of creating a multitude of confidential relationships among users—thus making confidentiality law a more attractive remedy to protect Internet users than other, vaguer, "privacy"-centered rules.

In an important article on the protection of digitized medical information, U.S. Department of Justice attorney Peter Winn defended the idea that confidentiality law can be a viable legal means to protect electronic health care information.[78] Winn observed that the federal Standards for Privacy of Individually Identifiable Health Information (the HIPAA Privacy Rules), which establish confidentiality obligations for health care providers, do not apply to "numerous [business associates] whose access to personal health information has exploded with the increased use of electronic health information."[79] The drafters of the HIPAA Privacy Rules recognized this problem[80]—which is endemic to all of confidentiality law—that downstream users of information are

---

[76] Citron, *supra* note 5, at 1850 (footnote omitted).

[77] Richards & Solove, *supra* note 5, at 178.

[78] *See generally* Winn, *supra* note 44 (advocating confidentiality law as a means of protecting medical records).

[79] *Id.* at 618.

[80] *Id.* at 651.

not bound by confidentiality. This flaw seemingly threatened to undercut the effectiveness of the HIPAA Privacy Rules.[81] After all, what good is it to require one recipient to maintain confidentiality if numerous other recipients are not bound to protect the same information?

According to Winn, the drafters were able to take advantage of a simple fact: "virtually all access by business associates to personal health information originates with healthcare providers and payers."[82] Based on this fact, the drafters created a prototype for this Essay's conception of chain-link confidentiality, which is addressed in greater detail in Part III. The HIPAA Privacy Rules provide that, although only covered entities such as healthcare providers are bound to confidentiality, these entities may not disclose information to their business associates without executing a written contract that places the business associate under the same confidentiality requirements as the healthcare providers.[83] According to Winn, since all health information "derives ultimately from healthcare providers who are in turn under a duty of confidentiality to the individual patient, the Rules thus put business associates under a contractual obligation that makes them agents of the covered entities . . . with the same duties of confidentiality."[84] This linking of parties creates a chain, and the law requires that privacy obligations follow information after an initial disclosure to a covered entity along that chain.[85]

This Essay proposes applying the logic similar to that employed by Winn and the developers of the HIPAA Privacy Rules to personal information online. Nearly all access by third parties to personal information on the Internet originates with two kinds of

---

[81] *See id.* ("[F]ailure to address the responsibilities of business associates within the system of disclosures of personal health information would vitiate the effectiveness of the [HIPAA Privacy] Rules themselves . . . .").

[82] *Id.*

[83] *Id.* (citing 45 C.F.R. § 164.504(e) (2001)). Congress recently amended HIPAA with the Health Information Technology for Economic and Clinical Health Act (HITECH). 42 U.S.C. §§ 17921–17953 (2006 & Supp. III 2009). HITECH amends the HIPAA Privacy Rules as an attempt to improve the privacy and security of electronic health information. Catherine Walberg, *How HITECH Are You? New HIPAA Privacy and Security Rule Requirements*, J. KAN. B. ASS'N, Sept. 2010, at 22, 23.

[84] Winn, *supra* note 44, at 651.

[85] *Id.*

entities: (1) Internet service providers (ISPs) and (2) software-based recipients, such as websites and software applications that utilize the Internet.[86] Because the original recipient of self-disclosed personal information on the Internet is largely discoverable[87]—via the website visited and the ISP used—a chain of confidentiality is possible. Although the number of potential recipients of personal information seems overwhelming, the reality is less daunting. Online, individuals have more opportunities for confidentiality, and they disclose information to fewer initial recipients, or "gatekeepers," than one might think.[88]

At its core, the Internet is a tool that connects people to one another and, perhaps just as importantly, to websites and entities. The core purpose of the most integral Internet feature, the hyperlink, is to connect one source to another. These connections all represent opportunities for confidential relationships and confidentiality agreements.

Although individuals disclose great amounts of personal information online, they disclose it to a surprisingly small number of websites. As a result, the majority of personal information on the Internet initially goes to a relatively small number of recipients. If confidentiality protections can effectively protect the

---

[86] *See The Tracking Ecosystem*, WALL ST. J., http://graphicsweb.wsj.com/documents/divSlider/ecosystemms100730.html (last accessed Dec. 17, 2011) (illustrating how tracking files log your online activity so that websites can provide individualized feedback and advertisements); Jennifer Valentino-DeVries, *How to Avoid the Prying Eyes*, WALL ST. J., July 31–Aug. 1, 2010, at W3 ("Visitors to almost every major website are tracked online."). This monitoring can occur through information submitted directly to a website or through the use of tracking technologies such as a cookie or beacon. *See* Julia Angwin, *The Web's New Gold Mine: Your Secrets*, WALL ST. J., July 30–Aug. 1, 2010, at W1 ("Beacons, also known as 'Web bugs' and 'pixels,' are small pieces of software that run on a Web page. They can track what a user is doing on the page, including what is being typed or where the mouse is moving."); Julia Angwin & Tom McGinty, *Personal Details Exposed Via Biggest U.S. Websites*, WALL ST. J., July 30–Aug. 1, 2010, at A1 ("The largest U.S. websites are installing new and intrusive consumer-tracking technologies on the computers of people visiting their sites—in some cases, more than 100 tracking tools at a time . . . .").

[87] *See, e.g.*, *Tracking the Trackers: Our Method*, WALL ST. J., July 31–Aug. 1, 2010, at W3 (explaining the methodology in analyzing the United States' fifty most popular websites for the presence of Internet tracking technologies).

[88] While cookies and other tracking technologies are used simultaneously with a visit to a website, this Essay does not treat them as the initial recipient of information since their legitimate installation is dependent upon a prior implantation by the visited website.

information held by that minority of websites, the lion's share of private information can be protected on the Internet.

The amount of information online is staggering.[89] Thankfully, under confidentiality law, the amount of information that is disclosed is largely not important. The focus is not *what* or *how much* is being disclosed, but rather, on *who* receives the disclosure.

Nielsen—a leader in consumer surveys on media consumption—estimated that the average Internet user visited around eighty-six domains in June 2010.[90] Even on a website likely to receive copious amounts of personal information, such as Facebook,[91] the average adult user has about 229 "friends."[92] Anyone with access to a profile receives that information from one source: Facebook. In this way, Facebook is similar to the covered entities under HIPAA as the source of personal information.[93]

Websites also collect personal information that an Internet user might not know is being disclosed, collected, or stored.[94] Websites

---

[89] According to Pingdom, an Internet monitoring company, 1.97 billion Internet users browsed 255 million websites and sent 107 trillion emails in 2010 alone. *Internet 2010 in Numbers*, PINGDOM (Jan. 12, 2011), http://royal.pingdom.com/2011/01/12/internet-2010-in-numbers/. Of course, 89.1% of the e-mails were spam. *Id.*

[90] *June 2010: Top Online Sites and Brands in the U.S.*, NIELSENWIRE (July 16, 2010), http://blog.nielsen.com/nielsenwire/online_mobile/june-2010-top-online-sites-and-brands-in-the-u-s/.

[91] Facebook is an Internet website where users interact with "friends." Friends are user profiles with whom the social network user shares a connection. *See* danah m. boyd & Nicole B. Ellison, *Social Network Sites: Definition, History, and Scholarship*, 13 J. COMPUTER-MEDIATED COMM. 210, 210–11 (2008) (describing the variations among social network sites). For example, one definition for social network sites, which are a type of online community, is "web-based services that allow individuals to (1) construct a public or semi-public profile within a bounded system, (2) articulate a list of other users with whom they share a connection, and (3) view and traverse their list of connections and those made by others within the system." *Id.* at 211.

[92] KEITH HAMPTON ET AL., PEW RES. CTR., SOCIAL NETWORKING SITES AND OUR LIVES: HOW PEOPLE'S TRUST, PERSONAL RELATIONSHIPS, AND CIVIC AND POLITICAL INVOLVEMENT ARE CONNECTED TO THEIR USE OF SOCIAL NETWORKING SITES AND OTHER TECHNOLOGIES 5 (June 16, 2011).

[93] *Cf.* 45 C.F.R. § 160.130 (2010) (defining covered entities under HIPAA).

[94] *See, e.g.*, Julia Angwin, *Latest in Web Tracking: Stealthy 'Supercookies,'* WALL ST. J., Aug. 18, 2011, at A1 ("Major websites such as MSN.com and Hulu.com have been tracking people's online activities using powerful new methods that are almost impossible for computer users to detect . . . ."). Researchers claimed that new techniques "reach beyond the traditional 'cookie,' a small file that websites routinely install on users' computers to help track their activities online. Hulu and MSN were installing files known as 'supercookies,' which are capable of re-creating users' profiles after people deleted regular cookies." *Id.*

use cookies[95] to collect information on the website's users, and websites may allow third parties to deploy third-party cookies as well.[96] The relationship between websites and third-party cookie users is yet another opportunity for confidentiality protections.

Websites that use cookies, Web bugs,[97] and other data collection technologies have access to a host of information, including comprehensive browsing and search histories, payment information, and contact information such as addresses, phone numbers, and e-mail addresses.[98] Solove and others have thoroughly documented the harms that can result from the disclosure of this information,[99] such as the compilation of a

---

[95] "Cookies are bits of encrypted information deposited on a computer's hard drive after the computer has accessed a particular Web site." SUSANNAH FOX, PEW INTERNET & AM. LIFE PROJECT, TRUST AND PRIVACY ONLINE: WHY AMERICANS WANT TO REWRITE THE RULES 7 (Aug. 20, 2000).

[96] *See, e.g.*, Matthew C. Keck, *Cookies, the Constitution, and the Common Law: A Framework for the Right of Privacy on the Internet*, 13 ALB. L.J. SCI. & TECH. 83, 89 (2002) ("An advertising company can use . . . any website . . . to set a cookie to a user's computer that can then be read across other websites and interact with the advertiser's web server. Because an advertiser's cookie is set when the user is visiting another entity's website, it is often referred to as a 'third-party cookie.' " (footnotes omitted)); *Tracking the Trackers: Our Method*, *supra* note 87, at W3 ("HTML cookies are small text files, installed on a user's computer by a website, that assign the user's computer a unique identity and can track the user's movements on a site. Flash cookies are used in conjunction with Adobe Systems' Flash software, which is widely used to display graphics and video on websites. Beacons are bits of software code on a site that can transmit data about a user's browsing behavior."). The problem of cookies should be separated from the more general problem of "spyware," which is "a broad term used to describe software that resides on a user's computer and monitors the user's online behavior." Richard G. Kunkel, *Protecting Consumers from Spyware: A Proposed Consumer Digital Trespass Act*, 28 J. MARSHALL J. COMPUTER & INFO. L. 185, 185 (2010). The larger issues of spyware usually involve complex issues of deceit and consent and are beyond the scope of this Article. *See also* Wayne R. Barnes, *Rethinking Spyware: Questioning the Propriety of Contractual Consent to Online Surveillance*, 39 U.C. DAVIS L. REV. 1545, 1545–48 (2006) (discussing whether contractual consent to continual surveillance should be unenforceable as a matter of public policy).

[97] Web bugs are similar to cookies in that they are "electronic tags that help Web sites and advertisers track visitors' whereabouts in cyberspace. But Web bugs are invisible on the page and are much smaller [than cookies]." Stefanie Olsen, *Nearly Undetectable Tracking Device Raises Concern*, CNET (July 12, 2000, 3:05 PM PDT), http://news.cnet.com/2100-1017-243077.html.

[98] *See generally* Angwin, *supra* note 86 (discussing the types of personal information collected by such devices).

[99] *See generally* SOLOVE, UNDERSTANDING PRIVACY, *supra* note 8; Hoofnagle, *supra* note 18 (describing privacy and due process risk where personal information is accessed and sold).

"digital dossier" that, if disclosed, could result in identity theft, government surveillance, wrongful denial of employment or insurance coverage, a chilling effect on speech or association, or emotional harm.[100]

This kind of sensitive, aggregated information has driven lawmakers, courts, scholars, the media, and the general public to call for greater privacy protections. The U.S. Senate, for example, has proposed a regulatory framework to minimize the collection of personal data, to improve constraints on the distribution of such data, and to maintain the accuracy of stored data.[101] The vast majority of the information this framework would protect online, however, would still come from two initial sources: ISPs and websites.[102] It would make sense, then, to fashion rules aimed squarely at these sources.

III. THE CHAIN-LINK CONFIDENTIALITY APPROACH

The general thesis of this Essay is that a chain-link confidentiality approach could be an effective way for the law to protect Internet users' personal information. While such protections should be supplemented by other laws, such as surveillance statutes[103] and privacy-related torts,[104] chain-link confidentiality could be a meaningful concept within a privacy protection regime. The previous section discussed the challenge of policing the downstream use of information and the promise of confidentiality on the Internet. This part will introduce the theory

---

[100] *See, e.g.*, Richards, *Information Privacy*, *supra* note 18, at 1097 (discussing the problems created by information disclosure, including identity theft); Daniel J. Solove, *The First Amendment as Criminal Procedure*, 82 N.Y.U. L. REV. 112, 148 (2007) (canvassing the potential negative results of public disclosure of personal information).

[101] Commercial Privacy Bill of Rights Act of 2011, S. 799, 112th Cong., Tit. III (2011).

[102] *See supra* note 86 and accompanying text. An ISP has been defined as a "firm in the business of providing Internet services to home or business customers, or sometimes other ISPs." JACK GOLDSMITH & TIM WU, WHO CONTROLS THE INTERNET?: ILLUSIONS OF A BORDERLESS WORLD 188 (2006).

[103] Electronic Communications Privacy Act (ECPA) of 1986, 18 U.S.C. §§ 2510–2522, 2701–2709 (2006).

[104] *See* RESTATEMENT (SECOND) OF TORTS §§ 652B–652E (covering the four privacy torts: intrusion upon seclusion, appropriation of name or likeness, publicity given to private life, and publicity placing person in false light).

of chain-link confidentiality and explore various methods of implementation.

A. THEORY

A chain-link confidentiality regime would allow for the limited disclosure of personal information as long as certain obligations to respect data followed the information as it was disclosed downstream. Chain-link confidentiality could be most useful to protect self-disclosed personal information. This is a notable strength. Perhaps the most significant failure of the application of privacy torts to the Internet is their failure to protect self-disclosed information. Unlike Samuel Warren and future Supreme Court Justice Louis Brandeis, who worried about tabloids publishing private moments,[105] the most likely publisher of personal information in the Internet age may be the user herself.[106] In light of the mass adoption of social media and the pervasiveness of electronically-mediated communication, Internet users seem to have become their own worst enemies.[107] Compounding this problem is the fact that Internet users often do not even realize that they are disclosing personal information.[108] Even if they do realize what they are disclosing, Internet users regularly feel like they have no choice or negotiating power when they disclose their personal information.[109]

---

[105] *See supra* note 77 and accompanying text.

[106] *See* James Grimmelmann, *Saving Facebook,* 94 IOWA L. REV. 1137, 1197 (2009) (discussing privacy issues regarding self-disclosed information on Facebook).

[107] *See, e.g.*, Julia Angwin & Steve Stecklow, *What They Know: A Wall Street Journal Investigation: 'Scrapers' Dig Deep for Data on Web*, WALL ST. J., Oct. 12, 2010, at A1 ("Many scrapers and data brokers argue that if information is available online, it is fair game, no matter how personal. 'Social networks are becoming the new public records,' says Jim Adler, chief privacy officer of Intelius Inc., a leading paid people-search website.").

[108] *See* Chris Hoofnagle et al., How Different Are Young Adults from Older Adults When It Comes to Information Privacy Attitudes & Policies? 17 (Apr. 14, 2010) (unpublished manuscript), *available at* http://ssrn.com/abstract=1589864 ("The entire population of adult Americans exhibits a high level of online-privacy illiteracy . . . ."); Ashkan Soltani et al., Flash Cookies and Privacy 4 (Aug. 10, 2009) (unpublished manuscript), *available at* http://ssrn.com/abstract=144682 ("Given the different storage characteristics of Flash cookies, without disclosure of Flash cookies in a privacy policy, it is unclear how the average user would even know of the technology.").

[109] *See, e.g.*, Tony Vila et al., Why We Can't Be Bothered to Read Privacy Policies: Models of Privacy Economics as a Lemons Market 1 (May 15, 2003) (unpublished manuscript),

Chain-link confidentiality can alleviate the tension between the disclosure and safety of personal information via a chain of protection. To create the chain of protection, contracts would be used to link each new recipient of information to a previous recipient who wished to disclose the information. These contracts would contain at least three kinds of terms: (1) obligations and restrictions on the use of the disclosed information, (2) requirements to bind future recipients to the same obligations and restrictions, and (3) requirements to perpetuate the contractual chain—i.e., to contractually obligate future recipients to continue the chain of contractual obligation if they wish to further disclose the information.

A number of optional elements could also be included in a chain contract, such as a requirement for documentation and a provision designating the subject or original source of the information as a third-party beneficiary. To that end, a basic chain-link confidentiality approach requires the same elements necessary to form a contract: mutual assent, capacity, and consideration.[110] This approach also requires some impetus to begin the chain of protection, either through statute, regulation, or voluntarily through an initial contract of confidentiality. If the three necessary elements of a chain contract are met, then ostensibly each new recipient of information will be bound by the same confidentiality as the initial recipient of information. Given the proper restrictions on use, this approach could protect an individual's privacy while still allowing for the dissemination of information online.

1. Obligations and Restrictions on the Use of Information. Restrictions on the use of disclosed information constitute the

---

available at http://www.eecs.harvard.edu/~greenie/econprivacy.pdf ("Others simply decide that loss of privacy is an inevitable consequence of doing business these days."); *Public Opinion on Privacy*, *supra* note 3 (explaining results of various polls of public opinion regarding online privacy); spde, Comment to *Are You Also Confused About Online Privacy?*, TELEFONICA PUB. POL'Y BLOG (June 8, 2011, 2:48 PM), http://www.publicpolicy.telefonica.com/blogs/blog/2011/06/08/are-you-also-confused-about-online-privacy/ ("Confused, yes! and also concerned! Concerned by the antiprivacy [sic] type of terms and conditions that most virtual services include in the contracts. . . . We want to be protected from abusive terms and conditions that we cannot negotiate.").

[110] *See* RESTATEMENT (SECOND) OF CONTRACTS §§ 12, 17, 18, 71 (1979) (defining the contracts concepts).

substance of a chain-link confidentiality regime. Here, the term "confidentiality" must be interpreted more broadly than a mere refrain from disclosing information. Instead, confidentiality should be construed, as one survey suggested, as "the obligation[ ] of individuals and institutions to use information under their control appropriately once it has been disclosed to them."[111] Indeed, to define confidentiality strictly as refraining from disclosure would not work in a chain-link confidentiality regime. The chain-link approach is designed to facilitate the limited sharing of information. It is important to emphasize, however, that the more restrictive conception of confidentiality would still be vital if a chain-link approach was adopted. Some information is so sensitive that it must be protected under the traditional and more protective laws regarding confidentiality agreements and confidential relationships. However, not all information on the Internet is this sensitive or must be protected so absolutely. Indeed, most personal information on the Internet is meant to be shared, but it still needs to be protected in some way.

This is where the flexibility of a chain-link confidentiality concept becomes useful. A number of obligations and restrictions could be incorporated into the chain contracts to protect an individual's privacy. Solove and Lecturer in Residence Chris Jay Hoofnagle have proposed a model regime of privacy protection based on notice, consent, control, and access.[112] These concepts could be incorporated as terms in chain contracts. These terms would then be the floor of protection for individuals whose information is being transferred. Responsible entities could always provide additional protections, but the level of protection would never drop below what was originally agreed upon for the initial disclosure or collection of information by ISPs and websites.

Chain contracts could prohibit further dissemination of personal information to particular parties, such as insurance companies. They could also require background checks and only

---

[111] Univ. of Miami School of Med., *Privacy and Confidentiality*, PRIVACY/DATA PROTECTION PROJECT (last modified May 12, 2005), http://privacy.med.miami.edu/glossary/xd_privacy_basicdef.htm.

[112] Daniel J. Solove & Chris Jay Hoofnagle, *A Model Regime of Privacy Protection,* 2006 U. ILL. L. REV. 357, 368.

permit sharing with "legitimate" organizations. An excellent example of such a restriction is included in the proposed Commercial Privacy Bill of Rights Act of 2011, which adopts a similar approach to the European Union Data Directive Safe Harbor (E.U. Data Directive) arrangement by prohibiting the transfer of data to "unreliable third parties."[113]

Indeed, the E.U. Data Directive, the U.S. Safe Harbor Arrangement,[114] the HIPAA Privacy Rules, and the proposed Commercial Privacy Bill of Rights provide numerous examples of obligations or restrictions that could be included in chain contracts, such as obligations of security, data integrity, access, transparency, accountability, and notification of breach.[115] The security requirement, for example, could obligate the recipient to keep the information secure from "unauthorized access, disclosure, alteration, and destruction."[116] Regarding data integrity, the contract could prohibit processing information in ways incompatible with the purposes for which it was originally

---

[113] Commercial Privacy Bill of Rights Act of 2011, S. 799, 112th Cong. §§ 302(a)(3), 302(b) (2011) (defining "unreliable third parties" as any entity that the discloser knows has violated a contract to protect information under the act or is "reasonably likely to violate such a contract"); *see also* Issuance of Safe Harbor Principles and Transmission to European Commission, 65 Fed. Reg. 45,665, 45,668 (July 24, 2000) (prohibiting the onward transfer of information to third parties that are not subject to the E.U. Data Directive or not bound by a written agreement providing at least the same level of privacy protection required by the relevant notice and choice principles); Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the Adequacy of the Protection Provided by the Safe Harbor Privacy Principles and Related Frequently Asked Questions Issued by the U.S. Department of Commerce 2000/520/EC, 2000 O.J. (L 215) 7, 8 [hereinafter Commission Decision] (finding that the U.S. Department of Commerce's Safe Harbor Privacy Principles provide adequate protection); 45 C.F.R. § 164.504(e)(2) (2011) (stating the requirements for business associate contracts).

[114] The U.S. Commerce Department has described the Safe Harbor arrangement as

> a mechanism, which, through an exchange of documents, enables the EU to certify that participating U.S. companies meet the EU requirements for adequate privacy protection. Participation in the safe harbor is voluntary. Organizations will need to adhere to the privacy requirements laid out in the safe harbor documents for all received from the EU.

Press Release, *Commerce Secretary William M. Daly Hails EU Approval of Safe Harbor Privacy Arrangement* (May 31, 2000), http://usinfo.org/wf-archive/2000/000531/epf306.htm.

[115] *See supra* note 113. Under the HITECH Act, covered entities must notify individuals of any breach of privacy regarding unsecured protected health information. 42 U.S.C. § 17932(a) (2006 & Supp. III 2009).

[116] Commission Decision, *supra* note 113, at 12.

collected.[117] This obligation could include a promise not to aggregate the data in a certain way or not to make the information available online or in certain formats.[118] A data integrity requirement could further require recipients to "take reasonable steps to ensure that [the transferred] data is reliable for its intended use, accurate, complete, and current."[119]

Terms in chain contracts could provide individuals with access to personal information about them along with an opportunity to correct or delete inaccurate information. Terms could also stipulate that notice be given to the individual regarding the use and onward transfer of her personal information.[120] To ensure that recipients of personal information have the infrastructure to comply with the requirements in a chain contract, terms could restrict transfer to those entities that have adequate managerial accountability, resources, and the capacity to respond to personal inquiries about the collection, use, transfer, or storage of personal information.[121] To properly trace the chain of information, contracts could require a centralized system of documentation of the transfer[122] and notification of any breaches of the terms to the subjects of the information.

Chain contracts could also stipulate that information only be shared if the collected data was anonymized, or that only certain kinds of data, such as addresses or information found on public profiles, could be shared. Privacy and information policy consultant Robert Gellman has proposed a statutory framework that utilizes a chain-link theory based on contractual agreements

---

[117] *See id.* (stipulating that "[a]n organization may not process personal information in a way that is incompatible with the purposes for which it has been collected").

[118] Such a promise could be seen as an attempt to preserve the obscurity of information. For more information on the benefits of online obscurity, see Hartzog & Stutzman, *supra* note 71.

[119] Commission Decision, *supra* note 113, at 12.

[120] *See id.* at 11 (incorporating such requirements in the E.U. Data Directive).

[121] *See* Commercial Privacy Bill of Rights Act of 2011, S. 799, 112th Cong. §§ 102, 401 (2011) (proposing accountability standards for entities that have information regarding a threshold member of individuals).

[122] *See id.* § 201(a) (requiring data collectors to maintain information "in a form that individuals can readily access"); Winn, *supra* note 44, at 651 ("The requirement of the existence of a contract between the covered entity and the business associate also ensures that the legal responsibility of the business associate with respect to confidentiality is properly documented." (footnote omitted)).

that mandate anonymization of personal information and impose prohibitions on reidentification.[123] Information sharing could be limited to third parties performing specific services or offering some benefit to the subject of the information.

The individual merits of these obligations and restrictions are beyond the scope of this Essay. Some terms will be more effective and less problematic than others.[124] Too many obligations and restrictions in a chain contract would unduly burden the flow of information. Too few would make the protection provided by the contract meaningless. Thus, the terms must strike a proper balance according to the context and proposed use of the information. In any event, it is clear that a variety of mechanisms currently exist to make chain contracts a flexible and meaningful privacy protection for individuals.

2. Similarly Binding Future Recipients. After establishing the initial recipient's obligations and restrictions on the use of personal information, the next step in a chain-link confidentiality approach is to ensure that those same obligations and restrictions will apply to future recipients of information. This step is accomplished through a contract that requires the new third-party recipient to agree to the same restrictions and obligations that bind the initial recipient of personal information. This is the first link in the chain of confidentiality.

Contracts are not the only means of linking privacy protections with information. Property-based theories of privacy,[125] as well as direct restrictions on the collection and use of certain types of information, also accomplish this goal. The use of chain contracts, however, is preferable to these other approaches for a few reasons.

Perhaps most importantly, confidentiality law is not as suspect under the First Amendment as other privacy remedies, such as the tort of public disclosure of private facts. In one of the most

---

[123] Robert Gellman, *The Deidentification Dilemma: A Legislative and Contractual Proposal,* 21 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 33, 47–49 (2010).

[124] *See, e.g.*, Reidenberg, *supra* note 20, at 733–34 ("Compliance with the national laws [stemming from the E.U. Data Directive] has also been an issue in Europe. The notice and registration requirements, in particular, appear to have a spotty reception.").

[125] *See, e.g.*, Samuelson, *supra* note 44, at 1125 (proposing an approach to privacy laws based on established trade secret laws addressing unfair competition); Schwartz, *supra* note 18, at 2056 (proposing a model of propertized personal information).

influential articles on the topic, Professor Eugene Volokh concluded that "information privacy rules are not easily defensible under existing free speech law."[126] Volokh was particularly troubled by the disclosure tort, which he saw as a content-based restriction on speech.[127] Other scholars have echoed this concern about the constitutionality of privacy remedies.[128] In response, the law of confidentiality has received significant support as a constitutional alternative to laws seeking to restrict the publication of certain kinds of information.[129] Richards and Solove found that there is "support for the proposition that existing First Amendment law is far more comfortable with enforcing nondisclosure rules in the context of relationships, even those involving the press."[130] Winn argued that "because the tort doctrine of breach of confidentiality does not create rights of privacy in information, itself, but protects information only in the context of well-defined relationships, it is likely to survive critical First Amendment review."[131] A contract-based system would also

---

[126] Volokh, *supra* note 37, at 1049; *cf.* Schwartz, *supra* note 72, at 1559 (describing Volokh's article as "the clearest expression that we have of the conflict between free speech and information privacy in the context of the First Amendment").

[127] *See* Volokh, *supra* note 37, at 1115–17 (expressing concern over the government passing regulations that restrict more information than necessary to protect sensitive private information).

[128] *See, e.g.*, Singleton, *supra* note 37, at 112–14 (noting that in privacy cases only false information is actionable under the First Amendment, which creates a problem for attempts to restrict publication of truthful information); Zimmerman, *supra* note 37, at 311–20 (describing the constitutional issues with punishing publication of truthful information).

[129] *See, e.g.*, Bezanson, *supra* note 44, at 1135 (advancing an enforceable obligation of confidentiality); Gilles, *supra* note 40, at 3 (suggesting that contract and fiduciary duty versions of a breach of confidence remedy could survive judicial scrutiny); McClurg, *supra* note 44, at 888 (proposing the existence of an implied contract of confidentiality in intimate relationships); Richards & Solove, *supra* note 5, at 173 ("[T]he First Amendment critiques that have limited the privacy torts in the United States would have much less force when applied to breaches of confidentiality."); Winn, *supra* note 44, at 621 (concluding that breach of confidentiality is likely to survive First Amendment review); Bibas, *supra* note 44, at 605, 609 (offering a contractual solution as a means of achieving more efficient privacy protection); Fast, *supra* note 44, at 433 (offering breach of confidentiality as a framework to build more effective privacy protections); Harvey, *supra* note 44, at 2392 (advocating an enforceable duty of confidentiality to protect privacy while staying within the bounds of the First Amendment); Vickery, *supra* note 44, at 1426 (developing a mechanism for the emerging breach of confidence tort).

[130] Richards & Solove, *supra* note 5, at 179 (footnote omitted).

[131] Winn, *supra* note 44, at 621.

be more voluntary than strict property or information-based approaches. Third parties that did not want to agree to the terms of the chain contract could simply refuse to enter into an agreement with the holders of personal information.

Contracts are also preferable to property- and information-based privacy restrictions because of the established body of law that can guide the development of the chain-link approach. A regime giving individuals a property right in their own information largely would be a new and untested system.[132] There already are a few examples of the chain-link approach in both European and American law. The E.U. Data Directive and the U.S. Safe Harbor Agreement have provisions requiring the use of contracts to bind third parties in the onward transfer of personal information.[133] The United States entered into the Safe Harbor Agreement to ensure compliance with the E.U. Data Directive's requirement that third countries could only receive personal information collected under the Directive if they provide an "adequate level of [data] protection."[134] The U.S. Safe Harbor Privacy Principles stipulate that organizations bound by the restrictions and obligations of the E.U. Data Directive are allowed to transfer information to a third party that is acting as an agent, but only if the organization

> first either ascertains that the third party subscribes to the [principles of the Safe Harbor Agreement] or is subject to [the E.U. Data] Directive or another adequacy finding or enters into a written agreement with such third party requiring that the third party provide at least the same level of privacy protection as

---

[132] *See* Pamela Samuelson, *Privacy as Intellectual Property?*, 52 STAN. L. REV. 1125, 1129 (2000) (identifying a property rights model as a theoretically "new form of intellectual property right in information").

[133] *See* Commission Decision, *supra* note 113, at 7 (demanding E.U. members transfer personal data to other countries only if assured of an adequate level of protection by those countries); Issuance of Safe Harbor Principles and Transmission to European Commission, 65 Fed. Reg. 45,665, 47,676 (July 24, 2000) ("[C]ompanies that want to avail themselves of the proposed 'safe harbor' will have to certify that they will protect the information they collect in accordance with prescribed guidelines.").

[134] Council Directive 95/46/EC, arts. 25–26, 1995 O.J. (L 281) 31, 45–46.

> is required by the relevant [principles of the Safe Harbor Agreement].[135]

Organizations that comply with the onward transfer requirements are not held responsible when a third-party recipient of information "processes it in a way contrary to any restrictions or representations, unless the organization knew or should have known the third party would process it in such a contrary way and the organization has not taken reasonable steps to prevent or stop such processing."[136]

As was previously mentioned, the HIPAA Privacy Rules also use a chain-link contract of confidentiality to allow limited disclosure while protecting information.[137] The U.S. Department of Health and Human Services issued these rules under the authority of the Administrative Simplification provisions of HIPAA.[138] According to Winn:

> Because the increased access to electronic personal health information increases the danger of harmful disclosure and misuse of that information, Congress, in enacting HIPAA, authorized federal regulatory protections for personal health information. The resulting Rules establish a federal floor of protections . . . [and] establish a set of fair information practices giving patients certain rights of notice, access, security, and consent with respect to disclosures of their personal health information that were not ordinarily provided under traditional common law doctrines of confidentiality.[139]

---

[135] *Safe Harbor Privacy Principles*, U.S. DEP'T OF COMMERCE, http://export.gov/safeharbor/eu/eg_main_018475.asp (last updated July 21, 2010).

[136] *Id.*

[137] *See* 45 C.F.R. § 164.504(e)(2) (2010) (requiring the business associate contract to establish "the permitted and required uses and disclosures of such [personal health] information").

[138] *See* 42 U.S.C. § 1320d-2(d)(2) (2006) (establishing safeguards for health information).

[139] Winn, *supra* note 44, at 618 (footnote omitted).

The HIPAA Privacy Rules originally applied only to healthcare providers, health plans, and healthcare clearinghouses ("covered entit[ies]").[140] These entities routinely need to share health information with others in the healthcare industry, such as business associates who provide "legal, accounting, administrative, management, and oversight services to healthcare providers and health plans."[141] In an innovative solution, the HIPAA Privacy Rules provide for the disclosure of health information by covered entities to business associates through the execution of a chain contract.[142] Specifically, "before a covered entity may grant access to personal health information to a business associate, the covered entity must obtain a written contract from the business associate promising to adhere to the same confidentiality standards as the covered entity."[143] In 2009, the Health Information Technology for Economic and Clinic Health Act (HITECH)[144] extended the HIPAA Privacy Rules to apply with equal force to a covered entity's business associates, such as vendors, drug companies, and insurance companies.[145] The HITECH Act's extension of protection is laudable, but as a general model for the protection of online information, it does not extend far enough.

The first draft of the proposed Commercial Privacy Bill of Rights[146] goes a step further and is perhaps the boldest attempt yet to create a chain-link confidentiality regime. Senators John Kerry and John McCain introduced this bill "[t]o establish a regulatory framework for the comprehensive protection of personal data for individuals."[147] One of the major provisions of this Bill is to give the FTC rulemaking authority to create privacy regulations and approve industry-created safe harbor programs.[148] The Bill would "generally require companies to notify consumers about the collection of their data, and also allow them to opt out of having

---

[140] 45 C.F.R. § 164.504(g)(1) (2010).

[141] Winn, *supra* note 44, at 618.

[142] *See* 45 C.F.R. § 164.504(e)(1)–(3) (2010) (setting forth the requirements for a contract between a covered entity and business associate).

[143] Winn, *supra* note 44, at 620.

[144] 42 U.S.C. §§ 17901–17953 (2006 & Supp. III 2009).

[145] *Id.* § 17931(a).

[146] Commercial Privacy Bill of Rights Act of 2011, S. 799, 112th Cong. (2011).

[147] *Id.* at pmbl.

[148] *Id.* § 201(a).

data used by third parties, like ad networks."[149] The Bill would provide for a number of other obligations and restrictions for covered entities, such as requirements to anonymize data in certain instances and to minimize the collection and retention of data.[150]

The provisions of the Bill most relevant to this Essay are in section 302, which details constraints on the distribution of information. Under this section, any covered entity seeking to distribute covered information must "require by contract that any third party to which it transfers covered information use the information only for purposes that are consistent with (A) the provision of th[e] Act; and (B) as specified in the contract."[151] Essentially, the required contract must bind any third-party recipients to the same obligations that bind the covered entity that originally collected the information.

However, the Bill goes further and requires that the chain contract must also prohibit the combination of unidentifiable information "with other information in order to identify" an individual without their consent.[152] As previously discussed, the Act would prohibit transfers to unreliable third parties and require that covered entities "assure through due diligence that the third party is a legitimate organization" and notify the FTC of any material violations of the contract.[153] Thus, the system of chain-link contracts provided for in the Commercial Privacy Bill of Rights not only extends the ground floor for privacy protections to third-party recipients of information[154] but also includes additional provisions to protect information. Although this Bill is still in draft form and subject to change, its initial iteration represents

---

[149] Wendy Davis, *Kerry Privacy Bill Could Impose 'Major' Obligations on Ad Networks*, ONLINE MEDIA DAILY (Mar. 23, 2011, 5:56 PM), http://www.mediapost.com/publications/article/147282/.

[150] S. 799 § 301. For a summary of the draft, see Christopher Wolf, *Draft "Commercial Privacy Bill of Rights Act of 2011" Published*, HOGAN LOVELLS CHRON. OF DATA PROTECTION (Mar. 23, 2011), http://www.hldataprotection.com/2011/03/articles/consumer-privacy/draft-commercial-privacy-bill-of-rights-act-of-2011-published/.

[151] S. 799 § 302(a)(1).

[152] *Id.* § 302(a)(2).

[153] *Id.* § 302(a)(3)(A)–(B).

[154] *Id.* § 302(c).

the most significant chain-link confidentiality approach to protecting privacy that lawmakers have articulated to date.

Chain-link contracts also have been used in other areas of the law, such as intellectual property. The "Share Alike" principle embedded in Creative Commons and open software licenses is a good example. Creative Commons is an organization offering a variety of copyright licenses that allow creators to choose the degree to which others may use their work and the terms on which it can be shared.[155] Under the Share Alike provision, copyright owners license others to do things like remix, tweak, and build upon their work in a non-commercial way, as long as the users of the work license their new creations under the identical terms stipulated by the original copyright owner.[156] Note that as long as the Share Alike provision is operative, there is no need to perpetuate the contractual chain because the intellectual property owners retain property-based rights. Thus, copyright owners do not have to rely upon a chain of contracts to assert the rights in their work against downstream users.

The breach of confidence tort is also capable of binding third-party recipients of information in the form of an "inducement" factor. For example, under the English law of confidentiality, a third party will be bound by the same obligation of confidence as an original confidant if the third party learned of the information through the confidant and took it with notice of its confidential nature.[157] Under English and American law, in some contexts, third-party recipients who induce confidants to breach their

---

[155] *About*, CREATIVE COMMONS, http://creativecommons.org/about (last visited Apr. 11, 2012).

[156] *About the Licenses*, CREATIVE COMMONS, http://creativecommons.org/licenses/ (last visited Apr. 11, 2012).

[157] *See* Campell v. MGN Ltd., [2002] EWCA (Civ) 1373 (2003) 1 Q.B. 633 at 662 (Eng.) (describing third party's duty of confidence when he receives information that he knows was disclosed in breach); Attorney Gen. v. Observer, Ltd., (1990) 1 A.C. 109 (H.L.) 268 (appeal taken from Eng.) ("The duty of confidence is . . . imposed on a third party who is in possession of information which he knows is subject to an obligation of confidence . . . ."); STANLEY, *supra* note 67, at 3–6 (explaining the basic principle behind the English law of confidentiality); Abril, *supra* note 6, at 716 (noting that English common law requires privity for contractual agreements to be binding); Richards & Solove, *supra* note 5, at 178 ("[A] third party can freely disclose private facts about a person as long as the third party did not learn the information from a confidant.").

obligation can be liable in tort to the original discloser or subject of the information.[158]

In a similar fashion, chain contracts would play a key role in the chain-link confidentiality approach by transferring a confidant's obligations to a third-party recipient. This approach is useful in contexts where extremely limited disclosure of personal information is necessary. However, as is discussed below, this approach must be modified to apply more generally to online information.

3. Perpetuation of the Contractual Chain. To make the chain-link confidentiality approach scalable to the entire Internet, it must accommodate the flow of information more than the traditionally restrictive confidentiality law and yet continue to protect information. To encourage the flow of information within a protected system, a chain contract must contain a provision that ensures the perpetuation of the contractual chain. Without such a provision, the chain-link confidentiality approach would limit the disclosure of information to only two parties: the initial recipient and any third parties to whom the recipient discloses information.

That approach alone could solve a number of problems regarding online privacy. In and of itself, the first two factors of chain-link confidentiality, restrictions and continuation of the restrictions, largely reflect our traditional confidentiality laws. The second factor, continuation of the initial recipient's restrictions, simply protects one additional level of disclosure—to encompass those in privity with the initial recipient of

---

[158] Winn, *supra* note 44, at 663–65. Winn analyzed a number of cases to ascertain the general rule in the health care context:

> [A] patient has a cause of action against a third party who induces a physician to breach his fiduciary relationship if the following elements are met: (1) the third party knew or reasonably should have known of the existence of the physician—patient relationship; (2) the third party intended to induce the physician to wrongfully disclose information about the patient, or the third party should have reasonably anticipated that his actions would induce the physician to wrongfully disclose such information; (3) the third party did not reasonably believe that the physician could disclose that information to the third party without violating the duty of confidentiality that the physician owed the patient; and (4) the physician wrongfully divulges confidential information to the third party.

Id. at 664–65.

information. This approach has already been effective in certain contexts, such as the protection of health information and the HIPAA Privacy Rules. Because the approach allows for a limited disclosure of the information to trusted third parties with a close relationship to the initial recipient, it provides the traditional strong confidentiality protections while accommodating the realities of electronic storage of health information and modern technology-based business practices.

On its own, however, the HIPAA approach restricts too much information to be generally applied across the Internet. The HIPAA Privacy Rules halt the flow of information and protections after two disclosures: the first, to the initial recipient, and the second, from the initial recipient to those working in privity with her. As a result, such a regime would offer little more than the "one off" protection provided by traditional confidentiality law. The HIPAA model may be desirable for sensitive health information that must be tightly controlled, but it would be unduly burdensome to recipients of information if applied to all personal information on the Internet. If personal information safeguards follow the information, online information should not be systematically and arbitrarily locked down after two levels of disclosure. Perpetuating the chain of contracts would facilitate the flow of data by continually re-creating an environment for sharing that accommodates the sender, receiver, and the subject of the personal information.

It is with this factor that the Commercial Privacy Bill of Rights excels as a model of chain-link confidentiality. In the initial draft, section 302(c)(1) provides that "a third party that receives covered information from a covered entity shall be subject to the provisions of this Act as if it were a covered entity."[159] This provision in essence converts all third-party recipients of covered information into covered entities.[160] Because all covered entities are obligated

---

[159] Commercial Privacy Bill of Rights Act of 2011, S. 799, 112th Cong. § 302(c)(1) (2011). The draft provides for some exceptions to this rule, including if the FTC finds that third parties cannot reasonably comply with the requirements of the Act or if the protections offered by the bill would not benefit the subject of the information if applied to the third party. *Id.* § 302(c)(2).

[160] Robert Gellman proposed a similar approach in a model statute for sharing and protecting deidentified personal information. *See* Gellman, *supra* note 123, at 52 (proposing

to bind third-party recipients to chain contracts, this provision effectively perpetuates the chain. If the chain of confidentiality remains intact, information could still be exchanged, yet the protections would follow. This could be an excellent compromise that would accommodate the sharing of information while protecting the downstream use of some personal data.

B. IMPLEMENTATION

Having developed the theory of chain-link confidentiality, this Essay now explores the various ways that it could be implemented. Most of the examples of employing chain contracts cited above have been created by statutes and international agreements.[161] However, a chain-link confidentiality regime could also be implemented through contract, tort, equity law, administrative regulation, or some combination of these.

The statutory approach exemplified by the Commercial Privacy Bill of Rights has numerous advantages. States could clearly provide the impetus for all three of the essential terms in the chain contract. Statutes also could create the general framework but delegate the particulars to administrative agencies that can more nimbly respond to technological change. As a civil rights issue, statutes would send a clear message that Congress, responding to public will, believes that the privacy of Internet users is indispensable. However, statutes are notoriously difficult to pass and amend. If the statute were not drafted correctly, it could

---

a statute allowing for voluntary data protection contracts where "[i]f allowed by the original data use agreement, the data recipient can become a data discloser with respect to the next recipient, and the protections continue in force because a new data use agreement is required" (footnote omitted)).

[161] S. 799 § 302(c)(1) (stating that "a third party that receives covered information from a covered entity shall be subject to the provisions of this Act as if it were a covered entity"); HIPAA Privacy Rules, 45 C.F.R. § 164.504 (2010) (requiring that those to whom various types of organizations transfer protected health information agree to the "same restrictions and conditions" that the organization agreed to); Issuance of Safe Harbor Principles and Transmission to European Commission, 65 Fed. Reg. 45,666, 45,668 (July 24, 2000) (stating that an organization wishing to transfer protected information to a third party must require the third party to comply with the Safe Harbor Principles by written agreement); Council Directive 95/46/EC, art. 7, 1995 O.J. (L 281) 31, 40 (only allowing processing of personal data if necessary to perform a contract to which the data subject is a party or "to take steps at the request of the data subject prior to entering into a contract").

create problems for Internet users, websites, ISPs, countless businesses, and the courts charged with administering the law.

The impetus for chain-link confidentiality might more effectively arise from a purely contractual approach. Websites might feel compelled to compete for a user's loyalty not only by promising to protect personal information but also by promising that protections would follow the website user's personal information downstream. A purely contractual approach also could be more flexible than a statutory one. Websites could craft protections based on the kinds of information that they collect and the design of the website or the services offered. A purely contractual approach could, in theory, better accommodate a website's business model as well as the users' expectations.

A purely contractual approach to chain-link confidentiality could also provide a benefit often absent from statutory schemes, including the proposed Commercial Privacy Bill of Rights: a private cause of action for the subjects of the information.[162] Such a right would have to be stipulated, however. By default, only the parties to a contract have a right to enforce their agreement.[163] In an online chain-link system, after the initial contract between an individual and a website, the parties to a contract would all be current and future recipients of information, leaving the individual powerless to enforce the chain contracts. The websites and recipients of information have little incentive to enforce these chain contracts if they are breached. After all, the confidentiality protections are for the benefit of the user, not the other contract adherents.

To make these contracts meaningful, the Internet user (and the subject of the information if they are not the same person) must be able to enforce the obligation of confidentiality anywhere along the chain. This can be done by requiring each chain contract to designate the Internet user as a third-party beneficiary to the

---

[162] *See* Wolf, *supra* note 150 ("No private rights of action are allowed [in the Commercial Privacy Bill of Rights] and state laws, except those dealing with health or financial information, data breach notification or fraud are preempted.").

[163] *See* 17B C.J.S. *Contracts* § 610 (1999) ("Generally, however, one who is not a party or in privity, and from whom no consideration moves, cannot sue for, or complain of, a breach of the contract, even though injured by such breach." (footnotes omitted)).

contract.[164] The Restatement (Second) of Contracts declares that "[a] promise in a contract creates a duty in the promisor to any intended beneficiary to perform the promise, and the intended beneficiary may enforce the duty."[165] So long as the chain contract makes it clear that the parties intend for the Internet user to have the right to enforce the contract, the law will honor that intent.[166]

Once the Internet user has been established as a third-party beneficiary, the user could bring an action based on two kinds of breach: (1) breach of a restriction on the information itself, such as a failure to anonymize information, or (2) failure to impose confidence upon another recipient of the information or failure to continue the contractual chain when transferring personal information.

A purely contractual approach would also have drawbacks. The initial contract between the website and the user would likely be standard form, which is a highly problematic area with respect to online privacy.[167] Users rarely read or understand the complex

---

[164] *See, e.g.*, Gellman, *supra* note 123, at 51 (stating that under current law, data subjects are unable to sue on a contract between a data discloser and a data recipient because of lack of privity).

[165] RESTATEMENT (SECOND) OF CONTRACTS § 304 (1981).

[166] *See id.* § 302(1) (noting that circumstances can indicate when the benefit of the promise is intended).

[167] *See* Barnes, *supra* note 96, at 1547–48 (highlighting the privacy problems spyware poses even though consumers often assent to spyware license agreements when they download other programs); Allyson W. Haynes, *Online Privacy Policies: Contracting Away Control over Personal Information?*, 111 PENN ST. L. REV. 587, 588 (2007) (stating that websites increasingly use privacy policies to limit their liability in how they share or sell individuals' information); Nancy S. Kim, *Clicking and Cringing*, 86 OR. L. REV. 797, 800 (2007) (observing that courts often find that consumers have assented to nonnegotiated software licenses even if they have not actually read the terms); Mark A. Lemley, *Terms of Use*, 91 MINN. L. REV. 459, 463 (2006) (noting that simply by using the Internet, employees of large corporations bind their companies to hundreds of different contracts with possibly inconsistent obligations); Andrea M. Matwyshyn, *Technoconsen(t)sus*, 85 WASH. U. L. REV. 529, 549–50 (2007) (discussing the communication problems associated with technology-mediated contracting contrasted with real space contracting, where parties negotiate face-to-face); Juliet M. Moringiello, *Signals, Assent and Internet Contracting*, 57 RUTGERS L. REV. 1307, 1315 (2005) (noting that courts apply the objective theory of contracts even with electronically-delivered terms despite the differences between paper and electronic communications); Nancy S. Kim, *'Wrap Contracts and Privacy* 1 (Ass'n for the Advancement of Artificial Intelligence Press Technical Report SS-10-05, 2010), *available at* http://ssrn.com/abstract=1580111 (observing that websites may take advantage of their customers' lack of knowledge of clickwrap and browsewrap agreements by inserting more aggressive and intrusive terms).

terms in these contracts.[168] Additionally, users are typically unable to negotiate terms with websites if they find the current terms unacceptable. Their only recourse is simply to walk away. Professor Paul Schwartz noted that "the phenomenon of 'bounded rationality' means that many consumers will accept whatever terms that data processors offer for their personal information. Behavioral economics scholarship has demonstrated that consumers' general inertia toward default terms is a strong and pervasive limitation on free choice."[169] Yet, given some novel approaches and a robust marketplace for privacy, a purely contractual approach to chain-link confidentiality is possible.[170]

Alternatively, the breach of confidence tort could be expanded to accommodate the chain-link system. Numerous scholars have called for greater recognition of this tort by courts.[171] The tort of breach of confidence has similar requirements to contracts of confidentiality, yet allows for a broader recovery of damages and is not so bound by the technical requirements of contract formation.[172] According to Richards and Solove:

> A plaintiff can establish a breach of confidence action by proving the existence and breach of a duty of confidentiality. Courts have found the existence of such a duty by looking to the nature of the relationship between the parties, by reference to the law of

---

[168] Joseph Turow et al., *The Federal Trade Commission and Consumer Privacy in the Coming Decade*, 3 ISJLP 723, 740 (2007) (reporting that only 1.4% of study participants reported reading the terms of standard-form electronic agreements often and thoroughly, 66.2% rarely read or browse these agreements, and 7.7% indicated that they have not noticed the agreements in the past or have never read them); Andy Greenberg, *Who Reads the Fine Print Online? Less than One Person in 1000*, FORBES (Apr. 8, 2010, 3:15 PM), http://www.forbes.com/sites/firewall/2010/04/08/who-reads-the-fine-print-online-less-than-one-person-in-1000/ (reporting that "just [0].11% of users click on a link to a site's terms of service").

[169] Schwartz, *supra* note 18, at 2081 (footnote omitted); *see also* Russell Korobkin, *Inertia and Preference in Contract Negotiation: The Psychological Power of Default Rules and Form Terms*, 51 VAND. L. REV. 1583, 1587–92 (1998) (noting bias in favor of default terms).

[170] *See, e.g.*, Woodrow Hartzog, *Website Design as Contract*, 60 AM. U. L. REV. 1635, 1639 (2011) (arguing that website features and design, such as privacy settings, should be considered enforceable promises in some contexts).

[171] *See supra* notes 5, 44.

[172] *See* Gilles, *supra* note 40, at 54–60 (noting that the tort of breach of confidentiality does not require a contract and allows recovery for mental suffering, injury to reputation, and punitive damages).

> fiduciaries, or by finding an implied contract of confidentiality.[173]

Like the purely contractual approach, a purely tort-based approach to chain-link confidentiality would require novel approaches and a robust privacy market. However, according to some, the tort of confidentiality could be used to supplement a statutory confidentiality scheme by providing a private cause of action absent from the statute. Winn concluded that this was the case for the HIPAA Privacy Rules because they "are likely to be adopted in private state actions for breach of confidentiality as establishing the duty whose breach is the predicate for the underlying tort claim."[174] Under this logic, depending on the wording, a statutory chain-link confidentiality scheme that does not provide for a private right of action could still form the confidential duty that serves as the basis for the breach of confidence tort. Given the flexibility of the common law, courts could expand the tort to apply to third-party recipients.

In addition to the "inducement" cause of action previously discussed,[175] courts could adopt the English law approach to confidentiality, which binds third-party recipients to an obligation of confidence if they knew or should have known the information they received was confidential.[176] The extension of confidentiality obligations to third parties could be recognized in equity as well.[177]

---

[173] Richards & Solove, *supra* note 5, at 157 (footnote omitted).

[174] Winn, *supra* note 44, at 619–20 (emphasis omitted).

[175] *See supra* notes 157–158 and accompanying text.

[176] *See* STANLEY, *supra* note 67, at 25. Stanley summarized the relevant English law as follows:

> A defendant who has not agreed to keep information confidential will have notice of its confidentiality sufficient to impose an obligation of confidence if, at the time of publication or use,
>
> (a) the defendant actually knows that the information is confidential,
>
> (b) it is obvious that the information is confidential, but the defendant willfully shuts his eye to that fact, or
>
> (c) on the facts as they are known to the defendant, a reasonable person would know that the information is confidential.

Id.

[177] *See id.* at 3 (finding that, historically, if a third party knew that disclosed information was something a discloser had agreed to keep confidential, then equity would impose a similar obligation on that third party); Abril, *supra* note 6, at 716 ("Under English law . . . a third party will owe an equitable obligation of confidence to the information's originator if

The doctrine of promissory estoppel is a flexible concept that enforces promises one detrimentally relied upon.[178]

Regardless of how chain-link confidentiality is implemented, such a system would not be a cure-all. Online privacy problems encompass more than the collection, use, and dissemination of personal information. Solove's taxonomy of privacy harms also includes what he calls "invasions" into people's private affairs, which need not involve personal information.[179] Depending on how a chain-link regime is crafted, it might only cover self-disclosed personal information, not information about individuals disclosed by third parties. For example, employers, directory services, media outlets, and a host of other websites post information about other people that they collect offline.

Not all information collected by websites is voluntarily disclosed to third parties. The practice of "scraping" websites using automated software to harvest data, while often a violation of a website's terms of service,[180] ostensibly would be difficult to police in a chain-link regime.[181] Moreover, not all self-disclosed personal information is disclosed online. Thus, a policy decision would need to be made as to whether a chain-link confidentiality regime would include all personal information or only information disclosed and collected online.

Additionally, this approach would cease to be effective once the chain is broken. Professor Patricia Sánchez Abril recognized this problem, stating: "When a contract governs the disclosure of information, the individual seeking protection is charged with obtaining the consent of everyone to whom the information is

---

the third party receives it with notice of its confidentiality." (footnote omitted)).

[178] *See* Hartzog, *supra* note 61, at 911–13 (discussing the doctrine of promissory estoppel).

[179] SOLOVE, UNDERSTANDING PRIVACY, *supra* note 8, at 105; *see also* Calo, *supra* note 19, at 1133 (describing one kind of privacy harm as subjective, that is, "the perception of unwanted observation," which "describes unwelcome mental states—anxiety, for instance, or embarrassment—that accompany the belief that one is or will be watched or monitored").

[180] *See, e.g.*, Register.com, Inc. v. Verio, Inc., 356 F.3d 393, 397 (2d Cir. 2004) (finding that Verio's solicitation of Register's registrants violated its terms of agreement); Pollstar v. Gigmania Ltd., 170 F. Supp. 2d 974, 977 (E.D. Cal. 2000) ("Pollstar further alleges that . . . [Gigmania] has downloaded concert information from [Pollstar's] web site [sic] and used the information for commercial purposes in breach of the [license agreement].").

[181] *See* Angwin & Stecklow, *supra* note 107, at A1 ("The emerging business of web scraping provides some of the raw material for a rapidly expanding data economy.").

disseminated. One break in the chain of trust is all it takes for the subject information to become freely distributable and viral."[182] While a cause of action could still lie with the party in breach, other remedies like the privacy torts, electronic surveillance statutes, and administrative regulations would be required to police those not in the chain of privity.

Even in light of these weaknesses, however, chain-link confidentiality could protect a lion's share of personal information on the Internet due to the concentration of our initial disclosures: ISPs and a handful of websites each day. Laws need not be perfect or perfectly enforced to be effective.[183] Indeed, as many have noted, the law, by itself, is not adequate to protect the privacy of Internet users. As noted by Professor Larry Lessig, social norms, systems design, and a robust marketplace must all be utilized for this goal as well.[184]

IV. CONCLUSION

Supreme Court Justice William O. Douglas wrote in a 1967 dissenting opinion that the authors of the Bill of Rights believed that "every individual needs both to communicate with others and to keep his affairs to himself."[185] He interpreted this to mean that "the individual should have the freedom to select for himself the time and circumstances when he will share his secrets with others and decide the extent of that sharing."[186] The need articulated by Justice Douglas is at the very heart of what is at stake regarding our privacy on the Internet. Individuals voluntarily and involuntarily disclose far too much personal information online to be subjected to complete transparency. While Internet use is a near necessity in modern society, its use leaves individuals

---

[182] Abril, *supra* note 6, at 715 (footnote omitted).

[183] *See, e.g.*, GOLDSMITH & WU, *supra* note 102, at 67 ("The law need not be *completely* effective to be *adequately* effective. All the law aims to do is to raise the costs of the activity in order to limit that activity to acceptable levels." (footnote omitted)).

[184] *See* LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE 85, 142–63 (1999) (arguing that the infrastructure of Internet "code" can help achieve a healthy balance between privacy and liberty online).

[185] Warden, Md. Penitentiary v. Hayden, 387 U.S. 294, 323 (1967) (Douglas, J., dissenting) (footnote omitted).

[186] *Id.*

vulnerable to privacy harms with little opportunity and few tools to protect themselves. Thus, it is critical to protect users' privacy online.

One of the most challenging aspects of this task is the protection of information once it is exposed to other people. This Essay has offered a theory of chain-link confidentiality as an approach to protecting online privacy. This approach could empower users to enforce their privacy rights as well as create an architecture for systemic privacy protection.

A chain-link confidentiality approach would use contracts to link disclosers and recipients of personal information. These contracts would contain at least three kinds of terms: (1) obligations and restrictions on the use of the disclosed information; (2) requirements to bind future recipients to the same obligations and restrictions; and (3) requirements to perpetuate the contractual chain. This theory is envisioned as a compromise allowing for greater dissemination of information than a strict confidentiality regime, while also providing more significant protection for users than the currently limited and often ineffective privacy laws.

Internet users might suspect their private information is broadcast to a nameless, faceless mass of strangers from the moment they log on. It is not, at least not at first. Users have relationships with ISPs and websites, with whom they disclose personal, often sensitive information. Users must trust websites with this personal information. Websites have relationships with third parties to whom they disclose that personal information or provide access to the user through the use of cookies and other data collection tools. These relationships also should be ones of trust.

The confidence that users place in ISPs and websites should not be destroyed by fear and suspicion brought by disclosure to third parties. Protections for personal information are largely ineffective if they are stripped the moment the recipient shares the information. Yet the collection and use of personal information is rapidly becoming the backbone of many extremely valuable Internet services. This is where chain-link confidentiality can alleviate the tension between confidentiality and the free flow of

information. The chain-link approach is one of protection and perpetuation within the context of relationships. By constructing a chain of protections that follow an Internet user's disclosure of information, courts and lawmakers could create a system that would provide meaningful privacy protection in an environment built for sharing.