Northwestern Journal of Technology and Intellectual Property

Volume 6
Issue 3 *Summer*

Article 1

Summer 2008

Health Privacy in a Techno-Social World: A Cyber-Patient's Bill of Rights

Patricia Sanchez Abril

Anita Cava

N O R T H W E S T E R N
JOURNAL OF TECHNOLOGY
AND
INTELLECTUAL PROPERTY

Health Privacy in a Techno-Social World: A Cyber-Patient's Bill of Rights

Patricia Sánchez Abril and Anita Cava

Summer 2008 VOL. 6, NO. 3

Northwestern Journal of Technology and Intellectual Property
Volume 6, Number 3 (Summer 2008)

Health Privacy in a Techno-Social World: A Cyber-Patient's Bill of Rights

Patricia Sanchez Abril[*] and Anita Cava[**]

¶1 Illness has long been the subject of denial, dread, and secrecy. Baring it reveals us at our most human and vulnerable. In a letter to a friend discussing his tuberculosis and hospitalization, Franz Kafka vented angst about his isolation and state of ignorance regarding his then-taboo condition. Although withdrawn by nature,[1] he seemed to find comfort in sharing his treatment and experiences with a friend. Kafka wrote:

> Dear Robert: Only medical matters—everything else is too involved, but my treatment—its only merit—delightfully simple. Against fever, liquid Pyramidon three times a day. . . . Against coughing, Demopon (unfortunately doesn't help). . . . Verbally I don't learn anything definite, since in discussing tuberculosis of the larynx everybody drops into a shy, evasive, glassy-eyed manner of speech. . . . Otherwise: A good room . . . [t]he place seems to be a great gossipers' nest from balcony to balcony; for the time being it doesn't bother me.[2]

Imagine Kafka today. Instead of a social outcast imprisoned in a sanitarium, Kafka would likely be online sharing his experiences with other cyber-patients on MyHealthSpace.com.[3] On this hypothetical website, he might create a digital health profile, replete with pictures, details of his prognosis, medication lists, lab results, family medical history, and daily journals chronicling his emotions. Our imagined cyber-Kafka would certainly find information, solace, and support in his ability to socialize with healthcare providers and other patients around the world. However, like the captive Kafka above, cyber-Kafka would have to contend with the privacy implications of

---

[*] Assistant Professor, Business Law Department, University of Miami School of Business Administration. Project HealthDesign ELSI Group. Support for work on this article was provided in part by a grant from the Robert Wood Johnson Foundation® in Princeton, New Jersey.

[**] Associate Professor, Business Law Department, University of Miami School of Business Administration. Project HealthDesign ELSI Group. Professors Abril and Cava would like to thank the Robert Wood Johnson Foundation® and UM Ethics Programs for their support and Kenneth Goodman, Michael Froomkin, and Reid Cushman for their insightful and thought-provoking conversations on this topic as part of the Project HealthDesign ELSI Group. The authors would also like to acknowledge the valuable research assistance of UM Ethics Programs Summer Research fellows Alissa Del Riego, Kristyn Medina, and Joshua Morales.

[1] Kafka once wrote: "I have often thought that the best mode of life for me would be to sit in the innermost room of a spacious locked cellar with my writing things and a lamp." *Letter from Franz Kafka to Felice Bauer (Jan. 14, 1913), in* LETTERS TO FELICE 156 (Erich Heller & Jurgen Born trans., 1973).

[2] *Letter from Franz Kafka to Robert Klopstock (Apr. 7, 1924), in* LETTERS TO FRIENDS, FAMILY, AND EDITORS, 1900–1924, at 411(Richard & Clara Winston trans., 1977).

[3] As of this writing, MyHealthSpace.com is a hypothetical illustration that combines common hallmarks of several existing websites, including but not limited to Google Health, Revolution Health, DailyStrength.org, HealthSpace (UK), and PatientsLikeMe.

interacting in a virtual "great gossipers' nest." Unlike gossip from "balcony to balcony," gossip from bits to bits introduces a modern set of privacy gambles.

¶2 In recent years, online social networking websites like MySpace, Facebook, and Second Life have changed the way many people communicate, socialize, and memorialize their daily lives. "Online social networking" refers to websites whose main purpose is to act as a connector between users via self-generated web profiles or avatars that represent the user's identity in cyberspace.[4] Online profiles are part diary, part autobiography, and part museum of the self.[5] Often displaying personal information and photographs, online profiles interact with other profiles to create a rich web of social connections.

¶3 Some have proposed that social media is ideal for health care.[6] Online health networking has been defined as "the use of social software and its ability to promote collaboration between patients, their caregivers, medical professionals, and other stakeholders in health."[7] Like social network profiles, online health profiles operate as a vehicle for healthcare recordkeeping and communication. The perceived benefits of online health networking have caused a rapid growth in websites devoted to health. Websites like Revolution Health, Organized Wisdom, Patients Like Me, and Google Health are revolutionizing the way patients share their health information and personal experiences, learn about health conditions, add to the body of scientific data, and socialize with other patients.[8]

¶4 As idyllic as this all may sound, this new technology may not be as healthy as it seems. On online social forums, the reward is also the risk: socialization through disclosure. While online fora might offer patients the comfort of a like-minded cohort, patients early to adopt the technology may be bartering their privacy with no legal or normative infrastructure to protect them. What if an employee of the website divulges a user's diagnosis to a newspaper, which publishes it to the world? What if another MyHealthSpace user tells the cyber-patient's employer of his condition? What if the cyber-patient's family members disapprove of online disclosure? What if the website goes out of business or expels the cyber-patient, and all of his health information is lost? What if the website sells the cyber-patient's medical identity to marketers or commercial data brokers?

¶5 Much ink is currently being devoted to analyzing the introduction of electronic or patient-controlled personal health records ("PHR") in the provision of health care.[9]

---

[4] *See* Patricia Sanchez Abril, *Recasting Privacy Torts in a Spaceless World*, 21 HARV. J. L. & TECH. 1, 13 (2007).

[5] *Id.* at 13-14.

[6] iHealthBeat.org, *Experts Call for Use of Social Media to Promote PHR Adoption*, IHEALTHBEAT, Mar. 20, 2008, http://www.ihealthbeat.org/articles/2008/3/20/Experts-Call-for-Use-of-Social-Media-To-Promote-PHR-Adoption.aspx. *See also* Jane Sarasohn-Kahn, *Trust Driving People to Web Social Networks for Health Info*, IHEALTHBEAT, Apr. 23, 2008, http://www.ihealthbeat.org/articles/2008/4/23/Trust-Driving-People-to-Web-Social-Networks-for-Health-Info.aspx.

[7] JANE SARASOHN-KAHN, THE WISDOM OF PATIENTS: HEALTHCARE MEETS ONLINE SOCIAL MEDIA 2 (2008), *available at* http://www.chcf.org/documents/chronicdisease/HealthCareSocialMedia.pdf.

[8] Matthew Holt, *MySpace for Healthcare? Much Closer Than You Think*, BIO-IT WORLD, Feb. 6, 2007, http://www.health-itworld.com/newsitems/2007/february/02-06-07-dhp-social-networking-in-healthcare.

[9] *See* MARKLE FOUNDATION, THE COMMON FRAMEWORK FOR NETWORKED PERSONAL HEALTH INFORMATION (2008), http://www.connectingforhealth.org/phti/ (establishing guidelines for safeguarding the confidentiality of online PHRs). SEE ALSO THE NATIONAL COMMITTEE ON VITAL AND HEALTH STATISTICS OF THE U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES, ENHANCED PROTECTIONS FOR

PHRs have been defined as "applications that enable individuals to collect, view, manage, or share their health information and conduct health-related transactions electronically."[10] Tech behemoths Google and Microsoft have recently introduced PHR platforms.[11] Governments around the world have begun hosting the online exchange of health information.[12] Following this trend, the U.S. government has commenced design of a nationwide, interoperable platform for electronic health information, which is slated for completion in 2014.[13]

¶6 Although related, privacy concerns stemming from online health networking websites are distinct from those identified in the existing PHR privacy debate, which to date has focused squarely on the unregulated relationship between the website operator or Internet service provider ("ISP") and the patient-consumer.[14] The many privacy risks posed by online health networking involve a complex web of real-life and cyber-relationships, questionable duties to the cyber-patient, and the technological capabilities to widely and permanently publish another's private information. Consequently, health networking privacy breaches can have several perpetrators: a malevolent blabbermouth, a mercenary web operator, a medical identity thief, or even an impulsive cyber-patient with a false sense of security.

¶7 By identifying the privacy challenges posed by online health networking and the areas of weakness in the law, this Article aims to evolve the legal and normative rubric governing privacy on this new techno-social medium. Section I begins by describing the phenomenon of online health networking and Section II posits its foreseeable challenges to personal privacy. Section III goes on to examine the extant legal infrastructure governing health privacy and queries whether this rubric properly protects privacy when translated to the online social arena. In light of the fact that the law is currently ill-equipped and norms are not yet established, it becomes necessary to formulate a stopgap solution. To that end, Section IV proposes a Cyber-Patient's Bill of Rights and

---

USES OF HEALTH DATA: A STEWARDSHIP FRAMEWORK FOR "SECONDARY USES" OF ELECTRONICALLY COLLECTED AND TRANSMITTED HEALTH DATA (2007), *available at* http://www.ncvhs.hhs.gov/071221lt.pdf (developing a framework for maintaining the privacy of health data transferred through secondary uses); SARASOHN-KAHN, *supra* note 7 (describing the nature of interactive online communities dedicated to user-generated health content).

[10] MARKLE FOUNDATION, *supra* note 9, § CP8, at 2.

[11] Michael S. Gerber, *New Ways to Manage Health Data; Giants Join the Push to Put Records Online*, WASH. POST, Mar. 11, 2008, at HE01.

[12] The United Kingdom's National Health Service has introduced "HealthSpace," a patient-controlled online health profile that promises to be an interactive central repository of health information. Michael R. Kidd, *Personal Electronic Health Records: MySpace or HealthSpace?*, 336 BRIT. MED. J. 1029 (2008). Australia and France offer other examples of government-based electronic medical record initiatives. *See Facilitating Coordinated Care for People with Chronic Health Conditions*, 8 HEALTHCLIX, May 2008, at 2, *available at* http://www.healthconnectsa.org.au/Portals/0/HealthClix%20May%202008.pdf; CHANTAL CASES & PHILIPPE LE FUR, ELECTRONIC MEDICAL RECORDS (2006), *available at* http://www.hpm.org/survey/fr/a8/3.

[13] The government-controlled health networking model brings to light additional privacy concerns above and beyond those inherent to their privately-funded and health-provider-controlled counterparts. Although beyond the scope of this article, such privacy concerns include the Fourth Amendment implications of having the government control a citizen's private health information. *See* THE WHITE HOUSE, A NEW GENERATION OF AMERICAN INNOVATION 8 (2004), *available at* http://www.whitehouse.gov/infocus/technology/economic_policy200404/innovation.pdf; U.S. GEN. ACCOUNTING OFFICE, PUBL'N NO. GAO-07-988T, HEALTH INFORMATION TECHNOLOGY: EFFORTS CONTINUE BUT COMPREHENSIVE PRIVACY APPROACH NEEDED FOR NATIONAL STRATEGY (2007).

[14] *See* MARKLE FOUNDATION, *supra* note 9.

Responsibilities. This "bill of rights" serves as a non-legal behavioral prescription for cyber-patients, website operators, and others. It begins to enumerate the multiple parties' duties to each other both on and offline. To date, no one has proposed a document governing relationships among cyber-patients interacting online and between these socializers and website operators. The Cyber-Patient's Bill of Rights and Responsibilities can therefore serve as a privacy imprimatur for cyber-patients, indicating a space where norms are defined and privacy is respected by all participating parties.

I. ONLINE HEALTH NETWORKING: TECHNO-SOCIAL MEDIA MEETS HEALTH CARE

¶8 Throughout history and across cultures, social networks have played a powerful role in influencing healthcare decisions, behavior, and even outcomes. Patient networks have provided advice, support, and counsel to the afflicted, due in large part to the accessibility, empathy, and willingness of participants to listen.[15] Health support networks have been instrumental in the promotion of health practices and specific interventions (such as breast cancer screening[16] and substance abuse referrals[17]). Social networks can also influence health-related behavior and mortality rates. Studies have shown individuals are much more likely to successfully quit smoking[18] or become obese[19] if their networks propagate these behaviors. A wide body of research also indicates that a supportive social network improves health outcomes for patients with a range of conditions, including postpartum depression[20] and heart failure.[21]

¶9 Today, the Internet has broadened the definition of community and social networks. Patients can now communicate with each other without regard for geography or proximity. Social media devoted to health has multiplied to include wikis, blogs, video-sharing, online forums, podcasts, and, of course, online social networks. Online social networks, such as MySpace and Facebook, invite users to participate in "groups," or public fora for people with similar interests to meet and interact.[22] As of August 2008, MySpace alone hosted 31,684 health-related groups.[23] The popularity of the social

---

[15] *See, e.g.*, Tom Ferguson, *From Patients to End Users: Quality of Online Patient Networks Needs More Attention than Quality of Online Health Information*, 324 BRIT. MED. J. 555 (2002); John Lester et al., *How Online Patient Networks Can Enhance Quality and Reduce Errors*, PATIENT SAFETY AND QUALITY HEALTHCARE, Oct.-Dec. 2004, *available at* http://www.psqh.com/octdec04/lesterfineganhoch.html.

[16] Jo Anne L. Earp et al., *Lay Health Advisors: A Strategy for Getting the Word Out About Breast Cancer*, 24 HEALTH EDUC. & BEHAV. 432 (1997). *See also* Jo Anne L. Earp & Valerie L. Flax, *What Lay Health Advisors Do: An Evaluation of Advisors' Activities*, 7 CANCER PRAC. 16 (1999).

[17] W. N. Leutz, *The Informal Community Caregiver: A Link Between the Healthcare System and Local Residents*, 46 AM. J. OF ORTHOPSYCHIATRY 678 (1976).

[18] Nicholas A. Christakis & James H. Fowler, *The Collective Dynamics of Smoking in a Large Social Network*, 358 NEW ENGLAND J. OF MED. 2249 (2008).

[19] Nicholas A. Christakis & James H. Fowler, *The Spread of Obesity in a Large Social Network Over 32 Years*, 357 NEW ENGLAND J. OF MED. 370 (2007).

[20] J. Hopkins & S. B. Campbell, *Development and Validation of a Scale to Assess Social Support in the Postpartum Period*, 11 ARCHIVES OF WOMEN'S MENTAL HEALTH 57 (2008).

[21] Steven L. Sayers et al, *Social Support and Self-Care of Patients with Heart Failure*, 35 ANNALS OF BEHAV. MED. 70 (2008).

[22] *See* MySpace Groups, http://groups.myspace.com/index.cfm?fuseaction=groups.categories (last visited Aug. 4, 2008).

[23] *See* MySpace Groups — Health-related, http://searchresults.myspace.com/index.cfm?fuseaction=groups.ListGroups&categoryID=17 (last visited

networking platform has also given rise to dedicated online health networks. PatientsLikeMe.com, for example, focuses on sharing health information for both emotional and research support.[24] Statistical data detailing such things as common symptoms, side effects, and drug dosages are generated from user-posted information. Users can then access the statistics, share advice, and receive feedback from other patients facing similar afflictions.[25] Other websites are dedicated to communities with specific conditions[26] or function as online support groups.[27]

¶10 Online health networks are capable of magnifying the proven benefits of physical-world networks for both patients and society in general. Cyber-patients can log in to read patient reviews on a medication or healthcare provider, glean information from others' experiences, and receive valuable decisional and emotional support.[28] Social media technology also offers the ability to easily update friends and family regarding recovery, prognosis, or post-operative status while limiting invasive queries.[29] Strong emotional support systems have been shown to have positive effects on recovery.[30] Health networking can also record, contextualize, and enrich personal medical histories. By interfacing with family members and linking health profiles, a rich, clinically-useful medical history can emerge.

¶11 Online health networking facilitates public health interventions, education, and conversations in novel environments and to new audiences. With the lure of a familiar communication medium, social media is being used to engage groups previously unengaged in their health care, such as teenagers.[31] The promise of anonymity on computer-based interfaces can promote open discussions about health status, behavioral risks, and fears while avoiding embarrassment.[32] One online health website acts as an authentication of the sexual health of potential sexual partners.[33] Users authorize their healthcare providers to upload the negative results of tests for common sexually transmitted diseases and then grant access to partners wanting proof of a clean bill of

---

Aug. 18, 2008) (this figure includes all groups falling within the Health, Wellness, Fitness category). There are over 500 health-related groups on Facebook.com. *See* Facebook Groups — Health-related, http://www.facebook.com (last visited May 21, 2008).

[24] *See* Patients Like Me, http://www.patientslikeme.com (last visited Aug. 10, 2008).

[25] *See* Thomas Goetz, *Practicing Patients*, N.Y. TIMES MAGAZINE, Mar. 23, 2008, at 32.

[26] *See* Life Raft Group, http://www.liferaftgroup.org (last visited Aug. 10, 2008).

[27] *See* Daily Strength, http://www.DailyStrength.org (last visited Aug. 10, 2008).

[28] *See, e.g.*, JUPITERRESEARCH, ONLINE HEALTH: ASSESSING THE RISKS AND OPPORTUNITIES OF SOCIAL AND ONE-TO-ONE MEDIA (2007) (finding significant percentage of adult online users in the United States not only connect to others or to information created by others online regarding health and wellness, but also use this information to make health-related decisions).

[29] *See, e.g.*, Margaret Buranen, *Want to Help? Log on to a Personal-help Website*, MIAMI HERALD, May 24, 2008, at 2E. *See also* Caring Bridge, http://www.caringbridge.org (last visited Aug. 10, 2008); Care Pages, http://www.carepages.com (last visited Aug. 10, 2008).

[30] Barbara Lantin, *Online, You Needn't Suffer Alone*, TIMES (London), Nov. 19, 2007, at 7.

[31] The New York City Health Department has launched a MySpace page called NYC Teen Mindspace for children and teenagers who are depressed or dealing with substance abuse issues. Visitors can obtain referrals for treatment by sending a confidential message to mental health counselors via the website's messaging system. *Health Department Gets MySpace Presence*, N.Y. SUN, July, 8, 2008, *available at* http://www.nysun.com/new-york/health-department-gets-myspace-presence/81401/.

[32] *See, e.g.*, Thomas N. Robinson et al., *An Evidence-Based Approach to Interactive Health Communication: A Challenge to Medicine in the Information Age*, 280 JAMA 1264 (1998); Jerome P. Kassirer, *Patients, Physicians, and the Internet*, 19 HEALTH AFF. 115 (2000).

[33] Check Tonight, http://www.CheckTonight.com (last visited Aug. 10, 2008).

health. Ongoing health conversations, such as those fostered by social media, have proven to improve overall health. A 2005 study concluded that publicity of a celebrity's breast cancer diagnosis increased the bookings for diagnostic mammograms and checkups in an "unprecedented" manner.[34] As a result of more information and continued healthcare conversations provided by social networks, the public is better equipped to make healthcare decisions and consider their implications.

II. PRIVACY CHALLENGES POSED BY ONLINE HEALTH NETWORKING

¶12 However enticing its benefits, online health networking can also pose significant challenges to personal privacy.[35] Health information reveals the most sensitive and intimate details of a person's life, such as psychological and sexual histories and private habits. Consequently, health privacy breaches have the potential to cause great harm with far-reaching effects ranging from loss of employment or insurance coverage to shame and stress that can further affect health. In fear of the possible repercussions of disclosures to unwanted audiences, privacy-wary patients may abstain from communicating via online health networks, thereby foregoing the many emotional and psychosocial benefits the medium may offer.

¶13 It is important to classify networking privacy breaches to grasp the technology, the reach of current privacy law, and whether legal redress is available or appropriate for each. Daniel Solove, noted privacy scholar, aptly defined and classified modern privacy violations in a coherent framework, which this Article borrows to understand the privacy concerns posed by online health networking. Professor Solove describes four general categories: (1) Information Collection; (2) Information Processing; (3) Information Dissemination; and (4) Invasion.[36] To these we add a fifth category indigenous to online networking: Self-exposure.

A. Information Collection

¶14 Information collection refers to the process of data gathering and can include surveillance, interrogation, or recording of an individual's activities.[37] It can be open or covert. It can occur in a private place or in public. On the Internet today, data gathering is the rule of the road. Internet users leave a trail of breadcrumbs with every mouse-click that forms part of their digital dossier. Many companies have volumes of personal information based on a recording of an individual's search patterns, personal preferences, and other online activity like emails.[38] For example, targeted advertising logs an

---

[34] Simon Chapman et al., *Impact of News of Celebrity Illness of Breast Cancer Screening: Kylie Minogue's Breast Cancer Diagnosis*, 183 MED. J. OF AUSTRALIA 247 (2005).

[35] Of course, other potential challenges exist in this new arena. One is the exacerbation of the digital divide into the healthcare arena, resulting in (perhaps) a sub-standard care for those without internet access. This and other non-privacy challenges are beyond the scope of this paper, but are certainly fodder for continued discussion.

[36] Daniel Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477 (2006).

[37] *Id*. at 491.

[38] *See* DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE 110 (Jack M. Balkin & Beth Simone Noveck eds., 2004) (identifying the influence of "an architecture that structures power, a regulatory framework that governs how information is disseminated, collected and networked" on protecting privacy).

individual's searches, clicks, and transactions to deliver ads of interest to the individual. When the practice is clear and consented to, targeted advertising may provide convenience and a comforting sense of familiarity to consumers. However, internet users currently have limited bargaining power to stop it, and little understanding or sense of its magnitude.[39]

¶15 Health information collection aggravates the potential for ensuing harm. Compare the consequences of capturing an individual's interest in spy novels versus his Viagra prescription or other medication from which a health condition can (correctly or incorrectly) be inferred. One report chronicled a woman's shock when she was barraged with ads for healthcare products after discussing her grandmother's recent death in a private email to her mother.[40] An advertising industry initiative has proposed guidelines for health-related behavioral targeting ads. In an awkward move to define topics properly designated as private, the proposal identifies certain health conditions and personal information deemed off-limits to ad targeting systems. These include cancer and psychiatric, sexual, and abortion-related conditions. Age, addictions, disability, marital status, pregnancy, beliefs, and affiliations are secondary topics the collection of which is left up to the discretion of the individual advertisers.[41]

B. Information Processing

¶16 Information processing describes the use, storage, and manipulation of collected data.[42] The category includes aggregation of information originally disclosed in multiple places, identifying an individual, secondary use, and exclusion. All of these identified harms are relevant in the health networking context.

1. Aggregation

¶17 First, aggregation is the bringing together of random pixels of personal information from multiple sources to paint what is often interpreted as a complete portrait of an individual. This necessarily involves removing each bit of previously-disclosed information from its original context, thus distorting the resulting image of the person. An overly simplistic caricature of an individual can result in dignitary and other harms and create a chilling effect. The controversy surrounding Robert Bork's video rentals is an early example of aggregation.[43] During his Supreme Court nomination hearings in 1988, Judge Bork's video rental log was obtained by a newspaper with the purpose of extrapolating conclusions on his personal views, tastes, and morals. The resultant public

[39] A recent Senate committee hearing emphasized the lack of public and legislative understanding about online data collection. Peter Whoriskey, *Senate Grapples with Web Privacy Issues*, WASH. POST, July 10, 2008, at D03.

[40] Louise Story, *Myth of Privacy Busted; Web Advertisers Scan E-Mails*, INT'L HERALD TRIB., Nov. 2, 2007, at Finance 13.

[41] Saul Hansell, *Ad Industry Ban Targeting People with Cancer; Ads to Widows and Orphans Allowed*, BITS: N. Y. TIMES TECHNOLOGY BLOG, Apr. 10, 2008, http://bits.blogs.nytimes.com/2008/04/10/ad-industry-bans-targeting-people-with-cancer-ads-to-dead-people-allowed/.

[42] *See* Solove, *supra* note 36, at 505.

[43] *Private Screenings*, ECONOMIST, Mar. 12, 1988, at 31.

outcry prompted Congress to pass the Video Privacy Protection Act,[44] which prohibits video rental companies from disclosing their clients' viewing preferences.

¶18 Today, anyone online can be Robert Bork, leaving clues to personal intellectual activity, interests, and beliefs scattered throughout cyberspace for any two-bit detective to unearth. As the reach of search engines expands and the data banks collected by separate websites coalesce, millions of people will gain access and draw inferences about an individual from the digital breadcrumbs disclosed on online networks. The potential risks for health-related information are obvious. As a Web pioneer recently quipped, "I want to know if I look up a whole lot of books about some form of cancer that that's not going to get to my insurance company and I'm going to find my insurance premium is going to go up by 5% because they've figured I'm looking at those books."[45]

2. Identification

¶19 A privacy violation can also occur by identification, connecting an individual's identity to information about him. Social networking websites allow users to use a pseudonym when interacting online. Some privacy-conscious internet companies are vowing only to sell or disclose de-identified user data, or non-personally identifiable information.[46] True anonymity, however, is an illusion and identification is not especially difficult, whether through use of the legal system or enterprising investigation. Website operators hold the key that connects the user to the information posted, either by tracking an Internet Protocol (IP) address or via login information. In a well-publicized civil copyright infringement case against YouTube, a court recently ordered the defendant to turn over its users' activity records, including their usernames and IP addresses, along with a detailed log of every video viewed.[47] This precedent opens the floodgates of the disclosure of networking user information. Under the court's reasoning, social networking websites such as YouTube may be compelled to disclose their users' screen names, computer locations, and public online activities, such as participation on public forums.

¶20 Even without a court order, fellow users and others can fairly easily reverse engineer online identities to disclose real-world personae.[48] In 2006, AOL released de-identified records of inquiries conducted through its search engine for academic research. Somehow, the records were released to the media and a reporter was able to figure out the identity of some of the users from the search records. The reporter contacted one user, who verified the information was hers and expressed concern that others might draw inferences from her searches for information on "bi-polar disorder."[49]

---

[44] 18 U.S.C. § 2710 (2000).

[45] Rory Cellan-Jones, *Web Creator Rejects Net Tracking*, BBC NEWS, Mar. 17, 2008, *available at* http://news.bbc.co.uk/1/hi/technology/7299875.stm.

[46] *See* Google Health Privacy Policy, http://www.google.com/health/html/privacy.html (last visited Aug. 10, 2008).

[47] Viacom International, Inc. v. YouTube Inc., No. 07 Civ. 02103, 2008 WL 2627388, at *5 (S.D.N.Y. July 2, 2008).

[48] "Reverse engineer" usually refers to the process of taking a machine or program apart to discover its inner workings and copy it. Here, I use the phrase to mean figure out someone's real identity.

[49] Michael Barbaro & Tom Zeller Jr., *The Face of AOL User No. 4417749: An Online Giveaway*, INT'L HERALD TRIB., Aug. 10, 2006, at 1.

3. Secondary Use

¶21 A secondary use breach occurs when information disclosed is used for purposes other than those originally intended by the user. For example, personal information and online viewing habits a user "makes public" to strengthen friendship ties may be sold to marketers or commercial data brokers by the ISP or website operator.

¶22 Personal health information disclosed on online health networking websites is at great risk for illicit transfer or sale, especially in light of its relative inaccessibility and its value to marketers. In response to market wariness, some online PHR providers have committed to not use patient information for commercial purposes[50] and to prohibit advertising banners on health profiles.[51] With most websites offering health networking services at no cost, it is unsettlingly unclear how these commercial ventures stand to make a profit in the absence of such commercialization. It remains to be seen how such commercial endeavors will thrive, if these promises are sustainable and legally enforceable, and whether cyber-patients will place their trust in these host corporations.

4. Exclusion

¶23 Exclusion is the failure to grant an individual's right to access his record and ensure its accuracy.[52] Many privacy laws, including the Privacy Act[53] and the Fair Credit Reporting Act,[54] protect individuals from exclusion by mandating transparency and granting access to records.

¶24 Online health networking, however, is free from any such regulation. Online networking websites grant users limited rights and little control over their individual profiles. While website operators usually claim no ownership or intellectual property rights over the information contained in a user's profile,[55] the websites' ability to delete user profiles and restrict their transferability to a competing networking website is tantamount to exercising proprietary and monopolistic control.

¶25 Many terms of use expressly grant the website operators authority to disable user accounts for any or no reason, and to delete all user information from the website without prior notice.[56] Participants in interactive websites who invest a substantial amount of time and money creating content on their profiles in reliance on a website's indefinite

[50] *See* Health Vault Privacy Policy, http://healthvault.com/HealthVaultPrivacy.htm (last visited June 3, 2008) (Microsoft leads consumers into the specific privacy policies with this four-part approach: "1. The Microsoft HealthVault record you create is controlled by you; 2. You decide what goes into your HealthVault record; 3. You decide who can see and use your information on a case-by-case basis; 4. We do not use your health information for commercial purposes unless we ask and you clearly tell us we may").

[51] *See* Google Health — Frequently Asked Questions, https://www.google.com/health/html/faq.html#data (last visited July, 10, 2008).

[52] *See* Solove, *supra* note 36, at 523.

[53] 5 U.S.C. § 552a(d) (2000).

[54] 15 U.S.C. § 1681g(a) (2000).

[55] *See, e.g.*, Patients Like Me — Terms and Conditions of Use, http://www.patientslikeme.com/about/user_agreement (last visited July 10, 2008); Revolution Health — Website Terms of Service, http://www.revolutionhealth.com/about/terms-of-service (last visited July 10, 2008).

[56] *See, e.g.*, Patients Like Me — Terms and Conditions of Use, *supra* note 55; Revolution Health — Website Terms of Service, *supra* note 55; MySpace Terms and Conditions, http://www.myspace.com/index.cfm?fuseaction=misc.terms (last visited Aug. 10, 2008); Facebook Terms of Use, http://www.facebook.com/terms.php (last visited Aug. 10, 2008).

service are understandably flabbergasted when expelled from a website without reason, explanation, or recourse.[57] This is especially true since most enforcement of terms of use seems arbitrary to website users, monitoring for violations of terms of use is rare, and examples of flagrant violations abundant.

¶26 Disabling an individual's profile often occurs without notice or an opportunity to appeal. Generally, operators can delete a person's account upon mere suspicion of wrongdoing and with little evidence. The websites are not required to disclose the reasons for deletion and do not have to grant a meaningful right of appeal.[58] In fact, most online networking websites have no procedures for reinstatement.[59] One recent case illustrates this tension. A music group's MySpace page, its main outlet for promotion and fan interaction, was taken down without notice, in effect erasing the band from existence.[60]

¶27 Unchecked member terminations may have serious repercussions when translated to the online health networking context. Losing access to one's online health profile can lead to erroneous diagnoses, loss of irreplaceable time in combating illness, and other more serious treatment issues. A breaching cyber-patient stands to lose his health record and support group, a devastating and disorienting proposition. PatientsLikeMe, for example, explicitly disclaims responsibility for the loss of information contained in a deleted health profile while establishing that a patient's membership may be terminated "with or without cause" and without prior notice.[61]

¶28 On the flip side, users wishing to permanently delete their networking profiles find it almost impossible to remove information linked to their profile such as tagged pictures, public comments on other profiles, and, of course, anything that has been sent to others.[62]

---

[57] One newsworthy example is that of Marc Bragg on Second Life. Mr. Bragg sued Second Life in 2006 for seizing around $4,000–$5,000 US of his virtual property when he was expelled from the website under the "any reason or no reason" clause of the Website's Terms of Service. The suit eventually settled and Bragg got his account and land reinstated. *See* Adam Reuters, *Linden Lab Settles Bragg Lawsuit*, REUTERS, Oct. 4, 2007, *available at* http://secondlife.reuters.com/stories/2007/10/04/linden-lab-settles-bragg-lawsuit/.

[58] *See* Contract Law section discussing ISPs Terms and Conditions and Privacy Policies *infra* notes 152–163 and accompanying text.

[59] As of August 2008, neither MySpace nor Facebook has specified any procedures for reinstating one's account post termination. *See* MySpace Terms and Conditions, *supra* note 56; Facebook Terms of Use, *supra* note 56.

[60] Michelle Henry, Gay Band Running Out of Space (Mar. 25, 2007), http://www.thestar.com/entertainment/article/195763 (with no specific explanation other than it had violated the website's Terms of Service, the band's MySpace page—its primary means of keeping in contact with their fans, friends, fellow musicians and business contacts—was deleted from the website).

[61] In its Terms and Conditions, PatientsLikeMe states: "You agree that PatientsLikeMe may, with or without cause, immediately terminate your PatientsLikeMe membership and access to the Member Area without prior notice. . . . *PatientsLikeMe has no obligation to maintain, store, or transfer to you information or data that you have posted on or uploaded to the Site."* Patients Like Me — Terms and Conditions of Use, *supra* note 55 (emphasis added).

[62] EUROPEAN NETWORK AND INFORMATION SECURITY AGENCY, SECURITY ISSUES AND RECOMMENDATIONS FOR ONLINE SOCIAL NETWORKS (2007), *available at* http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_pp_social_networks.pdf.

C. Information Dissemination

¶29 Another modern privacy violation is information dissemination. Professor Solove lists two information dissemination sub-categories highly relevant to the online health networking context: disclosure and breach of confidentiality.

1. Disclosure

¶30 Disclosure harms occur when others (who are not necessarily in a confidential relationship with the aggrieved) disclose truthful but private information generally deemed offensive and not of legitimate public concern. In common parlance, this is "TMI": *too much information*. The problem intensifies and the consequences multiply in the online context, due to the larger, uncontrollable scope of the audience and the permanence and searchability of digital information. Networking websites pose interesting disclosure risks of their own. In online social forums, personal information is the currency of choice. Its unfettered exchange exposes it to the high risk of reaching unintended audiences.

¶31 Indisputably, the unwarranted disclosure of health information can lead to embarrassment and shame. More concretely, the revelation of health information can lead to discrimination, the loss of insurance or employment, the denial of a mortgage, or the use of information as evidence in child custody disputes or personal injury lawsuits.[63] News media stories abound regarding improper disclosures of personal health information to an incalculable number of other people. Eli Lilly released the names of all subscribers to its Prozac information website.[64] Individuals in Florida taking Prozac daily received a free sample of Prozac Weekly in the mail, courtesy of the drug company and a local drug store, alerting everyone from family members to the mail carrier about their medical treatment.[65]

¶32 Online revelations are particularly troubling when they affect a third party who has not assumed the risk of interacting or disclosing online. An individual's health record reveals private information regarding family members' health or medical conditions. Last year, Nobel laureate James D. Watson became the first individual to publish his sequenced personal genome on a website.[66] The genome reveals risks for genetically-linked diseases such as cancer and Alzheimer's disease and other serious conditions. This has obvious implications for family members who may not have consented to the public disclosure of their genetic propensities.[67]

---

[63] JOANNE L. HUSTEAD ET AL., GENETICS AND PRIVACY: A PATCHWORK OF PROTECTIONS 11 (2002), http://www.chcf.org/documents/healthit/GeneticsAndPrivacy.pdf.

[64] Robert O'Harrow, Jr., *Prozac Maker Reveals Patient E-Mail Addresses*, WASH. POST, July 4, 2001, at E1. *See also* News Release, FTC, Eli Lilly Settles FTC Charges Concerning Security Breach (Jan. 18, 2002), *available at* http://www.ftc.gov/opa/2002/01/elililly.shtm.

[65] Adam Liptak, *Free Prozac in the Junk Mail Draws a Lawsuit*, N.Y. TIMES, July 6, 2002, at A1, *available at* http://query.nytimes.com/gst/fullpage.html?res=9C07E2DE1E31F935A35754C0A9649C8B63.

[66] Deborah Smith, *The Genome Let Out of the Bottle*, SYDNEY MORNING HERALD (Australia), June 7, 2007, at 12, *available at* http://www.smh.com.au/news/science/genome-let-out-of-the-bottle/2007/06/07/1181089203045.html; Erika Check, *James Watson's Genome Sequenced*, NATURE, June 1, 2007, *available at* http://www.nature.com/news/2007/070528/full/070528-10.html.

[67] *See* Susan M. Denbo, *What Your Genes Know Affects Them: Should Patient Confidentiality Prevent Disclosure of Genetic Test Results to a Patient's Biological Relatives?*, 43 AM. BUS. L.J. 561 (2006).

2. Breach of Confidentiality

¶33 Publishing health information without the consent of all affected parties poses serious medical and ethical concerns, and may also be a breach of confidentiality. When parties have a special relationship of trust or make an explicit promise, the law recognizes an obligation of confidentiality.[68] In addition to the disclosure's inherent harm, a breach of confidentiality violates trust, causes damage to the relationship, and reduces the likelihood its victim will share again.

¶34 The online social networking environment has brought about a sweeping change in its users' notions of intimacy, friendship, and confidentiality.[69] It eases the costs of communication and transforms friendship into a collecting hobby.[70] The very definition of friendship and its ensuing obligations are increasingly unclear on online social media. Consequently, the level of confidentiality users expect is almost impossible to assess without explicit requests or privacy settings.

¶35 The existing privacy settings implemented by popular social networking websites are insufficient in the health networking context. These allow users to select one setting for their entire profile—public or private.[71] Health information sensitivity is much more nuanced. A cyber-patient may feel comfortable with his urologist knowing he takes Viagra, but prefer to keep that information from his dermatologist and online cancer support group.

D. Invasion

¶36 Invasion is an intrusion into a private sphere, be it spatial (a hotel room or a bedroom) or intangible (one's private affairs or checking account). The mere existence of networked health information poses an increased risk of this type of privacy harm. In the online networking context, an intruder might spy or hack into another's private networking profile or otherwise access information not meant for his eyes. The digital environment lends itself to additional intrusions by corporate interests, employers, or other unwanted audiences. Sockpuppeting, for example, is the "act of creating a fake online identity to praise, defend, or create the illusion of support for one's self, allies, or company."[72] In addition to intrusion, this practice involves deceit, often by omission

---

[68] Neil M. Richards & Daniel J. Solove, *Privacy's Other Path: Recovering the Law of Confidentiality*, 96 GEO. L.J. 123, 125, 131 n.42, 180 (2007); 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, 1057–58 (2000) (explaining that contracts of confidentiality arise in situations where "people reasonably expect—because of custom, course of dealing with the other party, or all the other factors that are relevant to finding an implied contract—that part of what their contracting partner is promising is confidentiality").

[69] *See* AMANDA LENHART ET AL., TEENS AND SOCIAL MEDIA (2007), *available at* http://www.pewinternet.org/pdfs/PIP_Teens_Social_Media_Final.pdf. *See also* Joel Garreau, *Friends Indeed?*, WASH. POST, Apr. 20, 2008, at M01, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2008/02/18/AR200804800736.html; James Randerson, *Warning: You Can't Make Real Friends Online*, GUARDIAN (London), Sept. 11, 2007, Final Edition at 9, *available at* http://www.guardian.co.uk/technology/2007/sep/11/facebook.myspace.

[70] *See, e.g.*, Lenhart, *supra* note 69; Garreau, *supra* note 69.

[71] Facebook has recently launched an application addressing this issue. Facebook Principles, http://www.facebook.com/policy.php (effective Dec. 6, 2007) (last visited Aug. 8, 2008). *See also* J. D. Biersdorfer, *Staying Private on Facebook*, N.Y. TIMES, Jan. 17, 2008, *available at* http://www.nytimes.com/2008/01/17/technology/personaltech/17askk-001.html.

[72] Brad Stone & Matt Richtel, *The Hand That Controls the Sock Puppet Could Get Slapped*, N.Y. TIMES,

("*did I fail to mention I'm the CEO of the company I'm touting?*"). Generally, online networks do not offer mechanisms to verify a member's identity or sub-rosa agenda.[73] Uncovering sockpuppets requires a delicate balancing between the poster's right to anonymity and the other members' right to be free from invasion or deceit.

¶37 Similarly, nosy employers or insurance companies might discover information that influences important decisions based on a person's genetic predisposition family medical history, or behavior. Other uninvited audiences such as pranksters could wreak havoc on a health networking website by posting erroneous or misleading content, leading fellow users to experience unnecessary anxiety or even death.

E. Self-Exposure

¶38 A new category of privacy-related harm in the social networking context is caused by the over-disclosing user.[74] In other words, people violate their own privacy via facilitating technologies. More than 90% of teenagers are online.[75] Of those, over half participate in online social networking.[76] Media reports detailing the privacy-noxious behavior of teens with technology abound.[77] However, less than half of teens who post regularly on networking websites restrict access to their photographs and videos.[78]

¶39 Under a comforting illusion of safety, an over-disclosing user might upload or share information without regard for the digital information's transferability, malleability, and permanence. These users, most often minors, share more than they would in the physical world—posting information and pictures that eventually embarrass or haunt them and others.[79] The sensitive information can then be accessed by unanticipated audiences, including employers, neighbors, and others who deal in real world consequences. Such seemingly self-inflicted harms can have dire implications with respect to personal safety and reputation.

¶40 Fault for these privacy harms has been uniformly attributed to the users themselves.[80] After all, the argument goes: *online, a fool and his privacy are soon parted*. Yet the problem of self-exposure may not be so unilateral. It is well documented that the pre-frontal cortex area of the brain, the area controlling reasoning, logic, impulse control, and judgment, is less developed in adolescents and may only mature around age 25.[81] The underdevelopment of the brain's risk assessment in teenagers may account for

---

July 16, 2007, *available at* http://www.nytimes.com/2007/07/16/technology/16blog.html.

[73] At least one health network has adopted application processes to verify member identities. *See* Join the LRG, http://www.LifeRaftGroup.org/members_join.html.

[74] For an interesting and personal account of the effects of online over-disclosure, see Emily Gould, *Exposed*, N.Y. TIMES, May 25, 2008, at 32.

[75] Lenhart, *supra* note 69.

[76] *Id.*

[77] Stephanie Reitz, *Teens Are Sending Nude Photos Via Cell Phone*, MIAMI HERALD, June 4, 2008.

[78] Lenhart, *supra* note 69.

[79] Reitz, *supra* note 77.

[80] *See* Clemency Burton-Hill, *I Got 'Poked' 200 Times After Appearing on Question Time*, MAIL ON SUNDAY (London), June 24, 2007, at 64. *See also* Catherine Rampell, *What Facebook Knows that You Don't*, WASH. POST, Feb. 23, 2008, at A15.

[81] *See* Laurence Steinberg, *Risk Taking in Adolescence: New Perspectives From Brain and Behavioral Science*, 16 CURRENT DIRECTIONS IN PSYCHOL. SCI. 55, 56 (2007).

the fact that they simultaneously want privacy but fail to take affirmative steps to safeguard it.

¶41 The implications in health networking are unmistakable. A teenager disclosing her health information online may not be concerned by its dissemination, or even expect it to be private. She may not be able to envision the future consequences the information may have on her employment opportunities, medical insurance, and reputation. If some users are divulging under mistaken expectations of privacy (biological or otherwise), whose responsibility is it to educate them?

¶42 Despite numerous national and international warnings about online social networking websites,[82] the websites have not been active in protecting the privacy of their users and others. While the websites' terms of use generally prohibit invasions of privacy and other tortious conduct, users are not likely to read or understand these policies.[83] Further, there are virtually no mechanisms by which to solve user disputes and inadequate monitoring of website terms.

III. THE EXTANT LEGAL ENVIRONMENT

¶43 Health networking technologies have the potential to upend healthcare relationships between patients and physicians, hospitals, health plans, and pharmaceutical companies and be a transformative vehicle for health care. Yet questions about privacy on these networks loom. A patchwork of federal and state statutes, common law, and private contracts protect privacy interests in the United States.

A. Statutory Law

¶44 The Electronic Computer Privacy Act of 1986, the Children's Online Privacy Protection Act of 1998, and the Health Insurance Portability and Accountability Act of 1996 are three federal statutes that may address burgeoning issues in the area of online health networking. The year associated with each betrays a tenuous applicability to social media. Congress could not have foreseen the reach of social networking and the panoply of modern privacy challenges that would ensue. Any applicability of these laws in the health networking context is incidental to their ambit and original purpose.

1. Electronic Computer Privacy Act of 1986

¶45 The Electronic Communications Privacy Act of 1986 [84] ("ECPA"), an extension of the 1968 Wiretap Act,[85] prohibits the interception and knowing or intentional disclosure of information transmitted or stored by a wire, radio, electromagnetic, photoelectric, or

---

[82] *See, e.g.*, EUROPEAN NETWORK AND INFORMATION SECURITY AGENCY, *supra* note 62; Susan Kinzie & Yuki Noguchi, *In Online Social Club Sharing Is the Point, Until It Goes Too Far*, WASH. POST, Sept. 7, 2006, at A01; Internet 101 — Blog and Diary Web Sites, http://www.wiredsafety.org/internet101/blogs.html (last visited June 3, 2008).

[83] Only 4% of consumers read policies every time they visit a website, and only 16% read them frequently. Many more (40%) indicate that they only occasionally read the policies, while 22 percent rarely read them and 18% never read them. A SURVEY OF CONSUMER PRIVACY ATTITUDES AND BEHAVIORS (2001), *available at* http://www.bbbonline.org/UnderstandingPrivacy/library/harrissummary.pdf.

[84] 18 U.S.C. §§ 2510–2522 (2000).

[85] *Id.*

photooptical system.[86] It applies to actions by law enforcement and other governmental agencies, as well as public and private employers.[87] The statute covers any communication by a person who exhibits a reasonable expectation that the communication is not subject to interception.[88] The ECPA imposes criminal liability and creates a civil remedy, permitting the aggrieved to sue for declaratory relief, injunctive relief, damages, plus reasonable attorneys' fees.[89]

¶46 Accordingly, the ECPA seems to prohibit entities such as social networking websites from knowingly divulging the contents of any private electronic communication or posting. The exact confines of the prohibition, however, are dictated by the extent to which the user's behavior evinces a reasonable expectation of privacy. ECPA prohibitions do not apply to conduct authorized by the service provider or user. [90] Moreover, the statute's legislative history states that "a subscriber who places a communication on a computer 'electronic bulletin board,' with a reasonable basis for knowing that such communications are freely made available to the public, should be considered to have given consent to the disclosure or use of the communication."[91]

¶47 The ECPA only bars disclosure of the content of private communications. In other words, non-content information is fair game. For example, a transcript of a cyber-patient's posting on a private online support group may be protected, but not the fact the cyber-patient participated in an HIV support group. Given the abilities discussed above to aggregate and reverse engineer identity, the ECPA provides very little solace or redress for an aggrieved cyber-patient. Whether content or non-content information is disclosed, a health networker's privacy would be similarly compromised.

2. Children's Online Privacy Protection Act of 1998

¶48 The Children's Online Privacy Protection Act of 1998[92] ("COPPA") requires commercial websites to meet heightened privacy requirements when hosting children. The statute mandates prior parental consent before information can be collected from children under the age of thirteen. It also requires that websites interacting with minors have a privacy policy disclosing information-collection practices (including types of personal information collected, how it will be used, etc.) and provide a contact at the website.[93] Subject to certain exceptions, a website must obtain parental consent before collecting, using, or disclosing personal information about a child under thirteen.[94]

¶49 While COPPA is the strongest consumer privacy law, its effectiveness in the social networking arena is limited. The statute only protects minors under thirteen, leaving the great majority of social networking teens to fend for themselves. Moreover, COPPA

[86] 18 U.S.C. § 2310(12) (2000).
[87] *Id.*
[88] 18 U.S.C. § 2510(8) (2000).
[89] 18 U.S.C. § 2520 (2000).
[90] 18 U.S.C. § 2701(c) (2000).
[91] H.R. Rep. No. 99-647, at 66 (1986).
[92] 15 U.S.C. §§ 6501–6506 (2000).
[93] *Id.*; 16 C.F.R. § 312.4 (b).
[94] No consent is required when the child's information is used to respond directly to a one-time request from the child, when the information is used to obtain parental consent and is not maintained thereafter, or collection is necessary to protect the security or integrity of a website, to take precautions against liability, or to respond to judicial process, among other things. *See* 15 U.S.C. § 6502(b)(2)(A)-(E) (2000).

protects the child-user from predatory practices originating with the ISP or website operator, not from any other privacy violators.

3. Health Insurance Portability and Accountability Act of 1996

¶50 The Health Insurance Portability and Accountability Act of 1996 ("HIPAA") is fundamental to any discussion of health privacy.[95] Crafted in anticipation of electronic medical record technology, HIPAA acknowledges the need to protect patients from privacy violations at the hands of their health care providers. In the event of a healthcare-related privacy breach, patients might revert to privacy-protective behavior, such as giving inaccurate information in their medical history, or not seeking healthcare in the first place, thus affecting the quality of care and even personal wellbeing.[96] HIPAA addresses the potential fallout of health privacy harms by establishing a framework of duties among healthcare providers.

¶51 HIPAA is the most comprehensive piece of federal legislation governing privacy.[97] Adopted in 2002, HIPAA's Privacy Rule was designed to protect personally identifiable health information ("PHI") in an increasingly electronic medical record environment. Essentially, HIPAA addresses the retention, storage, transmission and exchange of PHI, defined as anything related to the "past, present, or future physical or mental health condition" in "any form or medium."[98] Medical records (both paper and electronic), personal communications, and electronic communications (email and faxes) are all subject to HIPAA's requirements.[99]

¶52 HIPAA's Privacy Rule requires certain entities to obtain patient authorization before sharing PHI. These covered entities include: (1) healthcare providers (doctors, nurses, pharmacists); (2) healthcare facilities (hospitals, clinics, stand-alone healthcare facilities); (3) health plans (HMOs, insurers, Medicare/Medicaid); and (4) health information clearinghouses (billing services, community health information systems).[100] As repositories of health information, these entities must take the necessary steps to ensure that access, use, and disclosure of PHI are handled appropriately.[101] Although only these particular entities are subject to HIPAA standards, each covered entity must

---

[95] Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104–191, 110 Stat. 1936 (codified as amended in scattered sections of 26 U.S.C. and 42 U.S.C.). For a thorough explanation on the HIPAA regulations, *see* University of Miami Privacy/Data Protection Project, http://privacy.med.miami.edu/glossary/xd_privacy_stds.htm (last visited Aug. 10, 2008).

[96] *See* Ralph Ruebner & Leslie Ann Reis, *Hippocrates to HIPAA: A Foundation for a Federal Physician-Patient Privilege*, 77 TEMP. L. REV. 505, 529 (2004).

[97] *See* HEALTH PRIVACY PROJECT: MYTHS AND FACTS ABOUT THE HIPAA PRIVACY RULE (2007), *available at* http://www.healthprivacy.org/usr_doc/Myths_and_Facts.pdf.

[98] 42 U.S.C. § 1320d (2000).

[99] Note that HIPAA's Security Rule, which facilitates the use of health information for the treatment and payment of healthcare, only covers electronic information. 45 C.F.R. §§ 164.302, 164.306. S*ee also* Sharona Hoffman & Andy Padurski, *In Sickness, Health and Cyberspace: Protecting the Security of Private Healthcare Information*, 48 B.C. L. REV. 331 (2007).

[100] 45 C.F.R. §§ 160.103, 164.501. *See also* Covered Entity Charts DHHS, http://www.cms.hhs.gov/HIPAAGenInfo/Downloads/CoveredEntitycharts.pdf; Sonia W. Nath, Note, *Relief for the E-patient? Legislative and Judicial Remedies to Fill HIPAA's Privacy Gaps*, 74 GEO. WASH. L. REV. 529, 537–38 (2006) (offering an illustration of these covered entities in an electronic health environment).

[101] S*ee* Inside the Fence: Legal Users of Your Medical Records, http://www.patientprivacyrights.org/site/DocServer/Zones_Chart.pdf?docID=881.

assure that its business associates—from transcribing to cleaning services—protect patient information. Patients also have the right to request that covered agencies reveal all parties who have seen the record for any reason other than treatment, payment, or healthcare operations.[102]

¶53 HIPAA's privacy protections are not particularly stringent. Violations of HIPAA may result in anemic civil fines of up to $100 per violation.[103] Criminal indictments under HIPAA, for which the Department of Justice has exhibited a recent interest, still number fewer than ten.[104] All covered entities may see a patient's health information if the purpose is connected to treatment, payment, and healthcare operations; there is no explicit restriction of a "need to know" or other reasonable limit.[105] Others may obtain access under expansive interpretations of the regulations. For example, certain institutions have interpreted the regulations to allow patient information such as names, addresses, and dates of treatment to be disclosed without authorization to business associates for fundraising purposes.[106] Further, covered entities are authorized, and sometimes obligated, to disclose certain health information without the patient's permission; these exceptions arise in the context of promoting certain "public health activities" including research and reporting disease, "public health surveillance [and] public health investigations."[107]

¶54 HIPAA's privacy protections also present procedural problems. HIPAA does not preempt more stringent state laws governing the privacy of health information.[108] This

---

[102] A number of exceptions are clearly carved out of the privacy rule, allowing disclosure without permission for public health and oversight purposes, domestic violence reporting, certain judicial and administrative proceedings, and law enforcement needs, including national security. 45 C.F.R § 164.512(b).

[103] Civil fines of $100 per violation to comply may be imposed on a covered entity, up to a maximum of $25,000 per year for multiple violations of the identical requirement in a calendar year. 42 U.S.C. § 1320d-5 (2000).

[104] *See* Press Release, U.S. Department of Justice, Nurse Pleads Guilty to HIPAA Violations (Apr. 15, 2008), *available at* http://littlerock.fbi.gov/dojpressrel/pressrel08/hipaaviol041508.htm (nurse who wrongfully disclosed personally identifiable health information for personal gain faces a maximum penalty of ten years in prison, a maximum fine of $250,000, or both).

[105] *See, e.g.*, Nicholas P. Terry & Leslie P. Francis, *Ensuring the Privacy and Confidentiality of Electronic Health Records*, 2007 U. ILL. L. REV. 681, 732–33 (suggesting patient confidentiality under HIPAA "would be better served if the data and its dissemination were subject to a default limitation based on necessity or proportionality").

[106] *See, e.g.* Elizabeth Fernandez, *6,000 UCSF Patient's Data Got Put Online*, SAN FRANCISCO GATE, May 2, 2008, *available at* http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2008/05/02/MNKE10DRGN.DTL; James D. Molenaar, *The HIPAA Privacy Rule: It Helps Direct Marketers Who Help Themselves to Your Personal Health Information*, 2002 L. REV. M.S.U.-D.C.L. 855 (2002).

[107] 45 C.F.R. § 164.512. As Reid Cushman notes in *Primer: HIPAA and PHRs*, (2007) (University of Miami Ethics Programs Working Paper, on file with author), Healthvault addresses this loophole in its Privacy Policies by qualifying its promise of complete control over all data in its repository:

> Microsoft may access and/or disclose your personal information if we believe such action is necessary to: (a) comply with the law or legal process served on Microsoft; (b) protect and defend the rights or property of Microsoft (including the enforcement of our agreements); or (c) act in urgent circumstances to protect the personal safety and welfare of users of Microsoft services or members of the public (emphasis added).

See HealthVault Privacy Policy, *supra* note 50.

[108] Forward-looking states can enhance HIPAA's privacy protections. For example, effective January 1, 2008, California's amended Confidentiality of Medical Records Act covers certain PHR products by broadening the definition of a covered entity to include: "[a]ny business organized for the purpose of maintaining medical information in order to make the information available to an individual or to a

often leads to confusion and compliance problems for business.[109] Some speculate that the lack of a private right of action for aggrieved patients leads to a degree of insouciance by covered entities.[110] Further, covered entities and patients themselves are confused about the exact parameters of the privacy requirements.[111]

¶55 As weak as HIPAA's privacy protection may be, the statute has heightened institutional awareness of patient rights and generated a degree of respect where little existed.[112] While no private right of enforcement exists, healthcare providers and institutions are mindful that a legal duty of care exists, one that theoretically could be privately enforced on a negligence theory.[113] While initial attempts have not been particularly successful[114], the heightened concern for privacy of health information may herald a new judicial sensibility in this regard.[115]

¶56 Questions regarding the reach of HIPAA to networking websites remain largely unexplored.[116] As with most privacy laws, HIPAA duties are premised on relationships. As such, it is necessary to analyze each health networking party's role and relationship with the cyber-patient to determine its ensuing HIPAA duties, if any.

¶57 The most common health networking host is commercial: a for-profit entity provides a platform and applications for user-generated content. These entities promise to hold patient information and provide a forum for patient-authorized exchange. Commercial health networking providers are most likely not subject to HIPAA.[117]

---

provider of health care at the request of the individual or a provider of health care, for purposes of allowing the individual to manage his or her information, or for the diagnosis and treatment of the individual." California Assembly Bill 1298 (Oct. 14, 2007), *available at* http://www.leginfo.ca.gov/pub/07-08/bill/asm/ab_1251-1300/ab_1298_bill_20071014_chaptered.pdf (codified as amended at CAL. CIV. CODE §§ 56.06, 1785.11.2, 1798.29, 1798.82).

[109] Peter A. Winn, *Confidentiality in Cyberspace: The HIPAA Privacy Rules and the Common Law*, 33 RUTGERS L.J. 617, 618–19 (2002). *C.f.* Corey A. Ciocchetti, *E-Commerce and Information Privacy: Privacy Policies as Personal Information Protectors*, 44 AM. BUS. L.J. 55, 88 (2007) (weakness of HIPAA is failure to preempt more restrictive laws, leading to compliance problems for business).

[110] *See* Nath, *supra* note 100 (noting reluctance of federal courts to infer a private right of action under the Privacy Rule and the fact that the federal government lacks the resources to adequately enforce).

[111] *See* MARKLE FOUNDATION, *supra* note 9, at 2. *See also*, Ilene Moore et al., *Confidentiality and Privacy in Health Care From the Patient's Perspective: Does HIPAA Help?*, 17 HEALTH MATRIX 215 (2007).

[112] Commentators note the flagrant disregard of patient privacy as being a catalyst for adoption of the privacy rule. *See, e.g.*, Tamela J. White & Charlotte A. Hoffmann, *The Privacy Standards Under the Health Insurance Portability and Accountability Act: A Practical Guide to Promote Order and Avoid Potential Chaos*, 106 W. VA. L. REV. 709, 720–22 (2004). *See also* Joshua D. W. Collins, Note, *Toothless HIPAA: Searching for a Private Right of Action to Remedy Privacy Rule Violations*, 60 VAND. L. REV. 199, at n.1–5 and accompanying text (2007).

[113] Charity Scott, *Is Too Much Privacy Bad for Your Health? An Introduction to the Law, Ethics, and HIPAA Rule on Medical Privacy***,** 17 GA. ST. U. L. REV. 481, 516 (2000).

[114] Nath, *supra* note 100, at 540–41 n.86–94 (federal courts are not allowing a private enforcement action under HIPAA); *but see* Collins, *supra* note 112 ("Thus, even though the Privacy Rule does not explicitly create a duty of confidentiality for tort liability, it may do so by implication.").

[115] Acosta v. Faber, 638 S.E.2d 246 (N.C. Ct. App. 2006) (referring to HIPAA as standard of care for medical practitioners to avoid a claim for failure to prevent unauthorized disclosures of patient treatment information).

[116] Rather than focusing on social networks, scholars and studies note HIPAA's problematic application to the electronic medical records environment in general. *See*, Terry & Francis, *supra* note 105 (HIPAA's approach to privacy and confidentiality of electronic health information does not suffice); Nath, *supra* note 100 (focusing on ECPA and possibilities of opt-in and opt-out opportunities for cyber-patients).

[117] Google Health Terms of Service, https://www.google.com/health/html/terms.html (last visited July 11, 2008) (noting that, according to Google, it is not a "covered entity" under HIPAA).

HIPAA could only apply if a network host were to be acting as a "clearinghouse." An online health network may be functioning as a health information clearinghouse if any of the sources or destinations of networked information is a covered entity, such as a physician or a pharmacy.[118] Despite these creative arguments, health network ISPs seem to be the square peg to HIPAA's round hole. As such, scholars agree: health records maintained on an online health network can be more easily leaked, sold, subpoenaed, or otherwise misused.[119]

¶58 Healthcare providers and insurance companies are also incorporating social media into the provision and management of health care. One prominent insurer has launched a healthcare community in Second Life, a virtual world where users interface with self-styled avatars.[120] At least one hospital has launched a fully interactive social network, allowing for patient-controlled information exchange with clinical care providers, researchers, public health authorities, and other patients.[121] Such health networking websites controlled by doctors, insurers, or other health care providers would come under HIPAA's purview, as one would assume the patient has authorized the use and retention of the information as part of an established health care relationship.

¶59 Many privacy breaches on social media occur at the mouse-clicks of fellow cyber-patients or are facilitated by the patients themselves. Individuals, however, are not covered entities under HIPAA. Health information under a patient's control falls outside of HIPAA's ambit. For example, health information stored by a patient on an online health profile—or even a personal filing cabinet — has no claim to privacy.[122] Similarly, health information shared with friends or family members is not protected.

B. Common Law

¶60 As a practical matter, the common law legal system is ill-suited to provide redress to the online networker. As with any lawsuit, bringing a case to court is costly and time consuming.[123] Suing for a privacy breach is often counter-productive, as it would definitely bring more unwanted attention to the damaging information and incorporate it into the public record.[124] One British case aptly illustrates this point. Max Mosley, a well-known figure in international auto racing, sued British tabloids for intrusion after they unearthed his penchant for Nazi-themed sadomasochism.[125] At public trial, Mr.

---

[118] REID CUSHMAN, PHRS AND THE NEXT HIPAA II (2008), *available at* http://www.projecthealthdesign.org/media/file/PHR_HIPAA2.pdf.

[119] *See* WORLD PRIVACY FORUM, PERSONAL HEALTH RECORDS: WHY MANY PHRS THREATEN PRIVACY (2008), *available at* http://www.worldprivacyforum.org/pdf/WPF_PHR_02_20_2008fs.pdf.

[120] Molly Merrill, *Cigna Rolls Out Virtual World Program Pilot for Healthcare*, HEALTHCARE IT NEWS, July 1, 2008, *available at* http://www.healthcareitnews.com/story.cms?id=9473&page=1.

[121] Indivo, a prototype social network hosted by the Children's Hospital of the Harvard Medical School, is a prominent example. News Release, Children's Hospital of Boston, Fully Patient-Controlled Medical Record Gets National Demo (Jan. 26, 2007), *available at* http://www.childrenshospital.org/newsroom/Site1339/mainpageS1339P1sublevel284.html.

[122] A. Michael Froomkin, *Forced Sharing of Patient Controlled Health Records* (2008) (unpublished working paper), *available at* http://www.projecthealthdesign.org/media/file/Forced-sharing.pdf.

[123] *See* Sanchez Abril, *supra* note 4, at 31.

[124] John F. Burns, *Trial About Privacy in Which None Remains*, N.Y. TIMES, July 9, 2008, *available at* http://www.nytimes.com/2008/07/09/world/europe/09mosley.html?pagewanted=1&_r=1&hp.

[125] *Id.*

Mosley was forced to recount the particulars and details of his fetish, as well as its effect on his health and family life.

¶61 In a privacy tort case, monetary damages are hard to prove, as they commonly involve unquantifiable injury to reputation and dignity. Remedies in equity such as injunction are unavailable. Further, jurisdictional issues may stymie a suit.

¶62 Even if a victim wanted to pursue a legal claim, there may be no one to sue. Often, the identity of the perpetrator is difficult to determine, since many online networkers operate with pseudonyms that can only be deciphered by the website operator via subpoena.[126] Victims of online privacy torts such as defamation or disclosure of private facts cannot obtain legal redress from the websites themselves. Section 230 of the Communications Decency Act of 1996 shields ISPs and other service providers from torts, including defamation or other injurious publication, committed by their users, unless the provider fails to take action after actual notice or has itself played an active role in developing the harmful content.[127] Courts have reinforced the applicability of Section 230 in the social networking context.[128]

1. Privacy Torts

¶63 Few legal rules protect the privacy of voluntarily disclosed health information. In the event privacy breaches were to occur, the aggrieved would likely be forced to rely on the state common law of privacy, whose applicability in the health networking context is questionable.

¶64 Substantively, tort law is no more comforting to the unwittingly exposed. Traditional privacy torts address traditional harms. The American Law Institute's Restatement (Second) of Torts[129] forms the well-accepted foundation of state privacy law in virtually every jurisdiction in the U.S. The Restatement only addresses those harms occurring in four ways—by intruding on the victim's private space ("Intrusion"), using his likeness in a commercial context ("Appropriation"), placing him in a false light in the public eye ("False Light"), or disclosing his secrets ("Public Disclosure").[130] Intrusion applies when information is uncovered in a furtive way from a place within which the victim has a reasonable expectation of privacy, such as a home or a hotel room.[131] The tort also clearly encompasses the activities of high tech Peeping Toms, as it covers

[126] It is important to distinguish this point from a related one made above regarding anonymity. In Section II, we argue privacy harms such as identification can easily occur by "reverse engineering" a poster's identity via a guessing game, thus rendering anonymity online somewhat of a fiction. Here, we are discussing the need to unmask the defendant with certainty in order to serve process. A perpetrator intending to hide behind anonymity or pseudonymity would likely take active, tech-savvy steps to make it difficult to identify him, whereas the conventional user is unlikely to put forth such effort.

[127] Communications Decency Act 47 U.S.C. § 230(c) (2006) ("[N]o provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.").

[128] One recent case held a popular social networking website immune from negligence claims for failing to prevent an adult user from contacting and assaulting a minor via its network. Doe v. MySpace.com, 474 F. Supp. 2d 843, 849 (W.D. Tex. 2007).

[129] RESTATEMENT (SECOND) OF TORTS § 652B (1977).

[130] RESTATEMENT (SECOND) OF TORTS § 652 (1977).

[131] Intrusion upon seclusion requires the plaintiff to show that the defendant (a) intentionally intruded, physically or otherwise, (b) on the solitude or seclusion of another or on his private affairs or concerns, and (c) in a manner highly offensive to a reasonable person. RESTATEMENT (SECOND) OF TORTS §625B (1977).

unwarranted sensory intrusions like eavesdropping, wiretapping, and visual or photographic spying.[132] Appropriation focuses on the unpermitted commercial use of a person's identity.[133] The tort of False Light addresses the publication of information that casts a person in a false light.[134] Finally, Public Disclosure applies when the plaintiff's private facts are publicly disclosed by the defendant in an unsanctioned manner. The tort requires the plaintiff to show that the defendant gave publicity to a private fact that is not of legitimate concern to the public, where such disclosure is highly offensive to a reasonable person.[135] It has traditionally been relied upon by patients who suffered from the unwarranted disclosure of their sensitive health information by third parties, such as newspapers or other media outlets.

¶65 The most common privacy harms in the online health networking context are those addressed by the torts of Intrusion and Public Disclosure, although neither tort has been successfully applied to activities occurring on online social networks. As such, in the world of online social media, privacy torts have become an anachronism. As evidenced by the lack of online privacy tort jurisprudence, the privacy panorama has changed and the harms enumerated above no longer fit the Restatement's stale rubric. Even when available to a plaintiff, these rights of action are severely debilitated by the nature of the online forum and the information breached.

¶66 The weakness of privacy torts online is due to a blurring of what is private, public, shameful, and newsworthy in an exposed online social world. The success of a privacy tort claim hinges on an assessment of the reasonableness of the victim's expectation of privacy in the space invaded or information disclosed. This determination is highly dependent on the nature of the space, the circumstances surrounding the information and its intrusion, the relationship between the parties, the technology, and the prevailing social norms.[136] In general, the law does not protect privacy in public or publicly-accessible places, even when the information whose protection is sought is sensitive in nature.[137] For example, one court examined whether patients who were videotaped while receiving emergency medical treatment had a legitimate expectation of privacy.[138] Their images were broadcast without their consent on a television show called "Trauma: Life in the ER."[139] The court dismissed the patients' privacy claim because the medical treatment was "open to public observation."[140] As such, the common law does not recognize an individual's per se right to privacy in his medical information.

---

[132] RESTATEMENT (SECOND) OF TORTS § 652B cmt. b., illus. 1–5 (1977).

[133] RESTATEMENT (SECOND) OF TORTS § 652C (1977).

[134] *See generally,* John W. Wade, *Defamation and the Right of Privacy*, 15 VAND. L. REV. 1093 (1962) (discussing the complex interrelationship of privacy rights); William D. Segal, Notes and Recent Decisions, *Is "False Light" Recognized in California? — Werner v. Times-Mirror Co. (Cal. 1961)*, 50 CAL.L.REV. 357 (1962) (analyzing judicial interpretation of "false light" privacy claims and arguing for limiting recovery in certain cases).

[135] RESTATEMENT (SECOND) OF TORTS §§ 652D, 652B (1977).

[136] *See* Sanchez Abril, *supra* note 4, at 16.

[137] RESTATEMENT (SECOND) OF TORTS § 652C (1977) ("No one has the right to object merely because his name or his appearance is brought before the public, since neither is in any way a private matter and both are open to public observation. It is only when the publicity is given for the purpose of appropriating to the defendants' benefit the commercial or other values associated with the name or the likeness that the right of privacy is invaded.").

[138] Castro v. NYT Television, 370 N.J. Super. 282, 297 (N.J. Super. Ct. App. Div. 2004).

[139] *Id.*

[140] *Id.*

¶67 As a general rule, if information has been voluntarily disclosed by a patient to anyone in a non-fiduciary capacity or is publicly available somewhere, it is no longer deemed "private" and therefore privacy torts do not apply.[141] This is fatal to any online privacy claim. For example, if a person has a skin disease that is immediately visible to anyone that sees him, tort law may not protect a subsequent disclosure of the particulars of the condition. Similarly, health information voluntarily disclosed by a cyber-patient to an online support group is not likely to be protected from subsequent dissemination to his employer or any other unwanted audience.

¶68 For a Public Disclosure claim to succeed, the information disclosed must also be shameful. Courts have widely acknowledged that Public Disclosure only protects health information when it consists of "unpleasant or disgraceful or humiliating illnesses"[142] or "hidden physical or psychiatric problems."[143] This significantly limits the privacy protection granted to health information. Courts have sustained Public Disclosure suits for the publication of such health information such as an unusual disease,[144] a sexually-transmitted disease,[145] a mastectomy,[146] fertility treatments,[147] and plastic surgery.[148]

¶69 Finally, to succeed on a privacy tort claim, the disclosed information must not be of public concern. If the health information disclosed is newsworthy or of public concern, the aggrieved is precluded from recovery in tort, as such recovery is preempted by the formidable First Amendment.[149] Courts have held a wide range of information to be newsworthy. In *Shulman v. Group W Productions, Inc.*,[150] for example, plaintiffs were non-public figures who were involved in a near-fatal car accident. A camera crew filmed plaintiffs' extrication from the car and their transport to the hospital in the helicopter and recorded the flight nurse's conversations with one of the injured plaintiffs. This videotape and sound track were then broadcast on a documentary television show without the plaintiffs' consent. Weighing whether the filming and subsequent disclosure was an

---

[141] RESTATEMENT (SECOND) OF TORTS § 652D (1977). *See also* Sipple v. Chronicle Publ'g Co., 201 Cal. Rptr. 665 (Cal. Ct. App. 1984) (holding that the fact that the plaintiff had confided to a group of people that he was a homosexual vitiated the matter's privacy); Nader v. General Motors Corp., 25 N.Y.2d 560, 569 (N.Y. 1970) ("Information about the plaintiff which was already known to others could hardly be regarded as private to the plaintiff."); Wilson v. Harvey, 842 N.E.2d 83 (Ohio Ct. App. 2005) (concluding that dissemination of the plaintiff's contact information on a flyer was not an invasion of privacy because the information circulated was on the university's website and accessible to anyone).

[142] RESTATEMENT (SECOND) OF TORTS § 652D (1997), cmt. b.

[143] Goerdt v. Tribune Entm't Co., 106 F.3d 215, 220 (7th Cir. 1997).

[144] Barber v. Time, Inc., 159 S.W.2d 291 (Mo. 1942) (concluding that taking a picture of a woman without her consent that exposed her overeating disorder and publishing it was a violation of her right to privacy).

[145] *See* Benz v. Washington Newspaper Publ'g Co., 2006 WL 2844896, n.15 (D. D.C. 2006) ("In one of defendant Bisney's Internet articles, a reference to herpes is made in relation to plaintiff's and Mark Kulkis' alleged romantic relationship. The Court observes that public disclosure of such a condition, which is a private fact, would be highly offensive to a reasonable person.").

[146] Miller v. Motorola, Inc., 560 N.E.2d 900 (Ill. App. Ct. 1990).

[147] Y.G. v. Jewish Hosp. of St. Louis, 795 S.W.2d 488 (Mo. Ct. App. 1990).

[148] *See* Vassiliades v. Garfinckel's, 492 A.2d 580, 590 (D.C. 1985).

[149] *See* Sean M. Scott, *The Hidden First Amendment Values of Privacy*, 71 WASH. L. REV 683 (1996) (analyzing the relationship of the privacy tort to First Amendment jurisprudence); 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. 1057 (2000). *See also* Sanchez Abril, *supra* note 4, at 166–67 and accompanying text (discussing Public Disclosure and the First Amendment).

[150] 955 P.2d 469 (Cal. 1998).

infringement on their privacy rights, the California Supreme Court concluded the broadcast was of legitimate public concern and their appearance in it bore a "logical relationship to the newsworthy subject of the broadcast."[151] Other examples of health information held to be newsworthy include a non-public figure's HIV-positive status as it related to a publicized malpractice lawsuit,[152] a woman's rape,[153] and an individual's unwanted sterilization.[154]

¶70 It has been established that health information is not protected by privacy torts if it is not inherently shameful, has been previously disclosed, or is newsworthy. Given the narrow interpretation of privacy torts and the nature of the Internet, the probability of a successful lawsuit in tort is remote.

2. Contract Law

¶71 In the wake of tort law's frailty, some have advocated turning to contract law to better shape the expectations and behavior of parties to confidential information.[155] While a suit in tort may reward the plaintiff for the foreseeable damages, emotional or otherwise, contract law may offer parties the ability of quieting the purported busybody. Unlike tort law, contract law offers injunctive relief to avoid ongoing harm.[156]

¶72 The terms of use of most online networking websites create a legal relationship between the service provider and its members and define the website's rules.[157] Privacy policies act as a warranty on the website's use and disclosure of user information. The enforceability of these agreements is dependent on whether their terms meet the classic requirements of a binding contract or are unconscionable or a violation of public policy. To date, these contracts are largely unregulated.

¶73 Using such contractual vehicles as privacy protectors raises several issues. The first is the difficulty of informed consent online.[158] Of course, consent validates a privacy breach; but, what of *informed* consent? The general lack of comprehensibility and user-friendliness of the terms of use makes informed consent burdensome and exasperating for the average website visitor.[159] As evidenced by numerous surveys, the majority of website users does not understand, access, or know the significance of privacy policies

---

[151] *Id.* at 478.

[152] Lee v. Calhoun, 948 F.2d 1162 (10th Cir. 1991).

[153] *See* Bartnicki v. Vopper, 532 U.S. 514 (2001); Florida Star v. B.J.F., 491 U.S. 524 (1989).

[154] Howard v. Des Moines Register and Tribune Co., 283 N.W.2d 289, (Iowa 1979) (despite personal and private nature of the procedure, information about conditions at a county home a matter of public record).

[155] *See* Eugene Volokh, *supra* note 149. S*ee also* Andrew J. McClurg, *Kiss and Tell: Protecting Intimate Relationship Privacy Through Implied Contracts of Confidentiality*, 74 U. CIN. L. REV. 887 (2006).

[156] RESTATEMENT (SECOND) OF CONTRACTS § 357 (1981).

[157] *See* Sharon K. Sandeen, *The Sense and Nonsense of Web Site Terms of Use Agreements*, 26 HAMLINE L. REV. 499 (2003).

[158] Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609, 1661–64 (1999) (discussing the legal fiction of consent in the context of the Internet, specifically the use of boilerplate consent forms that do not require user agreement before taking effect).

[159] Significant empirical evidence shows that users are often daunted by the legal and overly technical nature of online terms and conditions and privacy policies. Consequently, they often fail to fully read or understand the terms and assume that service providers are legally obligated to safeguard their privacy. *See* Joseph Turow et al., *The Federal Trade Commission and Consumer Privacy in the Coming Decade*, 3 I/S J.L. & POL'Y INFO SOC'Y 725 (2007).

and terms of use.[160] Many user contracts are written abstrusely or in a legalistic style, dissuading even the most punctilious consumer from taking time out of her online pursuit to carefully read and understand them. This issue is exacerbated when the user is a minor. Further, terms of use and privacy policies vary from website to website, making true understanding of each contract more difficult and impracticable, especially since most users visit several websites a day.

¶74 Website contracts are built on shifting sands. The professed ability of many operators to change terms of use at any moment and without prior notice leaves users in a constant state of uncertainty about their rights and privacy expectations. According to a Federal Trade Commission report, "[w]ebsites rarely provide information about when the current policies were created or updated and, if updated, exactly what changes were made. . . . They tell consumers that the policies will likely change and instruct them to check back frequently."[161] Such tactics put the privacy burden on users, who would need to closely compare previous (and now unavailable) versions of the agreement with the new one to assess the changes made and their probable impact.[162] Most health networking websites adopt this widespread practice.[163]

¶75 Confusing and misleading terms of use and privacy policies are beginning to catch the attention of the FTC, the states' attorneys general, and other government enforcers. The New York attorney general accused Facebook of fraud for failing to live up to the representation of a "trusted environment for people to interact safely."[164] The attorney general of New Jersey is investigating another online social network because its terms of use state it may remove offensive content that is abusive, obscene, or an invasion of privacy, but the website lacks the tools to report or dispute this material.[165]

¶76 Spotty enforcement and a lack of mechanisms for dispute resolution further weaken the power of contract law online. A contract is only as good as its observation and enforcement. Social websites generally have no system of dispute resolution processes

---

[160] A SURVEY OF CONSUMER PRIVACY ATTITUDES AND BEHAVIORS, *supra* note 83. *See also* Press Release, User Vision, Social Networking Sites Must Do More to Protect Their Child Users (Oct. 9, 2007), http://www.uservision.co.uk/resources/news/2007/social-networking-sites-must-do-more ("The investigation by web usability consultants at User Vision, one of Europe's leading independent user experience companies, found that Facebook, Bebo and MySpace all lacked targeted, clear information about online security for [those] under 18.").

[161] Sheila F. Anthony, Comm'r, Fed. Trade Comm'n, The Case for Standardization of Privacy Policy Formats, http://www.ftc.gov/speeches/anthony/standardppf.shtm (last visited Aug. 18, 2008).

[162] Andrew Jankowich, *EULaw: The Complex Web of Corporate Rule-Making in Virtual Worlds*, 8 TUL. J. TECH. & INTELL. PROP. 1, 46 (2006) (discussing the fact that terms and conditions can change at any time leaves the question of how a "participant might determine what changes have been made beyond the date of the original agreement without an extremely close reading").

[163] *See e.g.*, Patients Like Me — Terms and Conditions of Use, *supra* note 55, ("We reserve the right to modify this Agreement at any time, and without prior notice, by posting amended terms on this Site."); Revolution Health Terms of Service, http://www.revolutionhealth.com/about/terms-of-service ("We may change these Terms of Service at any time, as we deem appropriate.") (last visited May 26, 2008); Google Health Terms of Service, *supra* note 117 ("Google may change this agreement and will post the modified agreement. Your continued use of Google Health after the date of the modified agreement is posted will constitute your acceptance of the modified agreement.").

[164] Office of the New York State Attorney General Andrew M. Cuomo, Attorney General Cuomo and Facebook Announce New Model to Protect Children Online (Oct. 16, 2007), *available at* http://www.oag.state.ny.us/press/2007/oct/oct16a_07.html. *See also* Anne Barnard, *After Inquiry, Facebook Agrees to Tougher Safeguards*, N.Y. TIMES, Oct. 17, 2007, at 5.

[165] *See* Caitlin Millat, *Earn Your Degree in Online Bullying with College Gossip Web Site*, DAILY NEWS, May 11, 2008, at 26.

for disputes between users and no mechanism for appeal or defense from social network banishment. Defamation and privacy breaches are common occurrences in social media, surely exacerbated by users' perceived lack of accountability. Similarly, there are scant appropriate forums for airing disputes against the website itself. Case law seeking to enforce terms of use is practically nonexistent. The only likely recourse for a cyber-patient seeking redress against a misbehaving website is to seek action by the FTC or the states' attorneys general[166] or under a private right of action under state unfair competition laws.

¶77 In the absence of trust and enforcement mechanisms, confidentiality agreements are the most reliable vehicles to protect the unwarranted disclosure of private health information.[167] American courts have consistently upheld the principle of "freedom of contract," generally allowing contracting parties to strike any bargain they wish, including confidentiality agreements.[168] These agreements have also been upheld against First Amendment challenges.[169]

¶78 Some scholars have argued that implied contracts of confidentiality can arise from romantic relationships or friendships.[170] Members of online health social networking websites form relationships based on trust and intimacy. They divulge private information pertaining to their health and emotional state assuming it will not be disseminated outside their perceived confined network.

¶79 Online, express confidentiality agreements are a more tenable solution. Facilitated through available technology, confidentiality agreements between users could assure a higher level of protection for those sharing private and personal information. In some instances, confidentiality agreements have been offered through online health ISPs as a prerequisite to membership. PatientsLikeMe.com includes such a clause as part of its terms of use. It states:

> You agree not to disclose to any person or entity personally identifiable information about other members that you learn using this Site (whether posted in the Member Area by a member or emailed to you by a member) without the express consent of such member. You may disclose information of a general nature (that could not identify the member who provided such information or

[166] *See, e.g.*, Federal Trade Commission, FTC Testifies on Social Networking Sites (June 28, 2006), http://www.ftc.gov/opa/2006/06/socialnetworking.shtm; Office of the New York State Attorney General Andrew M. Cuomo, *supra* note 164; State of New Jersey Office of the Attorney General, State Subpoenas Records from JuicyCampus.com As It Investigates the College Gossip Website (Mar. 18, 2008), http://www.nj.gov/oag/newsreleases08/pr20080318b.html. *Cf. Canada's Privacy Commissioner Launches Facebook Probe after Law Students File Complaint*, INT'L HERALD TRIB., May 31, 2008, *available at* http://www.iht.com/articles/ap/2008/05/31/business/NA-GEN-Canada-Facebook-Probe.php.

[167] Eugene Volokh, *supra* note 149, at 1057–58 (2000) (explaining that implied contracts of confidentiality arise in situations in which "people reasonably expect—because of custom, course of dealing with the other party, or all the other factors that are relevant to finding an implied contract—that part of what their contracting partner is promising is confidentiality").

[168] *See, e.g.*, Snepp v. United States, 444 U.S. 507 (1980); Jordan v. Knafel, 823 N.E.2d 1113, 1119–21 (Ill. App. Ct. 2005).

[169] *See* Cohen v. Cowles Media Co., 501 U.S. 663 (1991); Immunomedics, Inc. v. Doe, 775. A.2d 773 (N.J. App. Div. 2001).

[170] Andrew J. McClurg, *Kiss and Tell: Protecting Intimate Relationship Privacy Through Implied Contracts of Confidentiality*, 74 U. CIN. L. REV. 887, 912–17 (2006).

> whom such information is about) to third parties outside this Site, subject to the above restriction on non-commercial use.[171]

Confidentiality clauses could be both preventive and prescriptive. Clearly establishing the "rules of the road" between participating parties may deter disclosures before they occur as well as provide some redress after the damaging information is disseminated.

IV. CYBER-PATIENT'S BILL OF RIGHTS AND RESPONSIBILITIES

¶80 *Start with what is right rather than what is acceptable.*[172]

¶81 Given the awkwardness of the law in the social media context, one might conclude the only way of protecting privacy is to refrain from sharing personal information online. Rejecting such extreme measures, this Article sets out a framework of principles intended to provide a foundation for much-needed legislation or a meaningful self-regulatory system. Acknowledging the glacially slow pace of the legislative process vis-à-vis the dramatically nimble nature of the techno-social environment, it is necessary to articulate clear principles and recommendations to inform law, industry standards, and behavioral norms. To date, despite FTC recommendations for the enactment of stringent online privacy laws,[173] legislators have been slow to respond to privacy concerns posed by health networking.[174] Industry efforts to implement an effective self-regulatory system have failed.[175] Certification systems granted by overseeing third parties have proven to be the most successful at increasing privacy compliance on the part of the service providers.[176] But service providers are only one piece of the puzzle: cyber-patients must

---

[171] Patients Like Me — Terms and Conditions of Use, *supra* note 55.

[172] GUSTAV JANOUCH, CONVERSATIONS WITH KAFKA 56 (Goronwy Rees trans., 1971).

[173] In 2000, the FTC voted three-to-two to recommend that Congress enact legislation to ensure adequate protection of consumer privacy by requiring all consumer-oriented websites that collect personal identifying information to establish privacy policies in accordance with the four "Fair Information Practice Principles" ("FIPP"). The four FIPP identified by the FTC are "Notice and Awareness," "Choice and Consent," "Access and Participation" and "Security and Integrity." FEDERAL TRADE COMMISSION, PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE: A REPORT TO CONGRESS 36–38 (2000), *available at* http://www.ftc.gov/reports/privacy2000/privacy2000.pdf.

[174] To date, Congress has proposed but has not enacted two health information technology bills: the Wired for Healthcare Quality Act, S. 1693, 110th Cong. (2007) and the Health Information Privacy and Security Act, S. 1814, 110th Cong. (2007). The former expands the scope of HIPAA to cover "operator[s] of a health information electronic database." The latter addresses security issues to promote protection of sensitive information and grants individuals control over the use and disclosure of their protected health information. The Health Information Privacy and Security Act also protects a number of other important interests, such as an individual's right to amend his protected health information and be notified if his information is lost or compromised.

[175] In 2000, the FTC's third report concluded that self-regulatory initiatives had "fall[en] far short of broad-based implementation of effective self-regulatory programs." FEDERAL TRADE COMMISSION, *supra* note 173, at ii. *See also* FEDERAL TRADE COMMISSION, BEHAVIORAL ADVERTISING: MOVING THE DISCUSSION FORWARD TO POSSIBLE SELF-REGULATORY PRINCIPLES (Dec 2007), *available at* http://www.ftc.gov/os/2007/12/P859900stmt.pdf (again proposing principles to guide self-regulation to address privacy concerns).

[176] TRUSTe is one example of a web site security certification that is respected worldwide. TRUSTe is an independent organization whose mission is to build users' trust and confidence in the Internet. The TRUSTe privacy program is based on a branded online seal, the TRUSTe "trustmark." TRUSTe: Advancing Privacy and Trust for a Networked World, http://truste.org/about/mission_statement.php (last visited Aug. 10, 2008). It is awarded to websites that adhere to TRUSTe's privacy principles and agree to comply with its oversight and consumer resolution process. Companies joining the TRUSTe privacy

be held accountable for their actions regarding their personal information as well as that of others.

¶82 To that end, this Article proposes a Cyber-Patient's Bill of Rights and Responsibilities to systematically anticipate, address, and organize a set of norms and rules for the online health networking environment. This Bill of Rights and Responsibilities is predicated on a set of overarching principles supporting its legitimacy and credibility: (1) the balancing of paternalism and autonomy; (2) education and engagement of cyber-patients; (3) trust in the system, in technology, and in the community of users; and (4) a duty to respect other users.

¶83 Healthcare ethics has long understood the need to balance paternalism with patient autonomy. Education of health network users is necessary to achieve this balance, *ergo* the medical community's emphasis on information and consent. Trust in the social-media system—the websites, the underlying technology, and the community of users—is paramount to the spirit of the rights and responsibilities proposed below.

¶84 Finally, and perhaps most importantly, a duty to respect fellow users is fundamental in the world of online health networking. Cyber-patients often visit health networking websites in vulnerable states because of a medical condition. The responsibility of users to respect all fellow cyber-patients allows everyone to benefit from the use of the network without the additional burden of privacy concerns.

¶85 Building upon these basic principles, our Cyber-Patient's Bill of Rights and Responsibilities proposes to address the absence of law or "clear, consensus-based policies and practices"[177] to protect user privacy. Currently, service providers and cyber-patients act within a "moral free space"[178] regarding online health information. As described above, the online exchange of health information involves an unusual intersection of business, health, and private actors and results in a web of complex relationships and responsibilities. It thus becomes necessary to enumerate expectations, rights, and responsibilities.

A. Rights of Cyber-Patients

1. Right to an Effective Architecture of Privacy

¶86 Cyber-patients must have the right to the latest "systems for health information exchange [that] protect the integrity, security, and confidentiality of [their] information."[179] Health networking providers must offer the latest technological resources to protect user information from being used, accessed, or divulged in an

program must agree to inform users of the website of what personal information is being gathered, how it will be used, with whom it will be shared, and whether the user has an option to control its dissemination. TRUSTe Oversight, http://www.truste.org/about/compliance_monitoring.php (last visited Aug. 10, 2008). Based on such disclosure, users can make informed decisions about whether or not to release their personally identifiable information (such as credit card numbers) to the website.

[177] *See* MARKLE FOUNDATION, s*upra* note 9, at 6.

[178] THOMAS DONALDSON & THOMAS W. DUNFEE, TIES THAT BIND: A SOCIAL CONTRACTS APPROACH TO BUSINESS ETHICS (1999). *Moral free space* allows various individuals and communities to establish differing values and norms that are entitled to some presumption of validity. *Id*. at 41–42. However, the moral free space is not boundless, and the diversity of norms has its limits—acting as a boundary to "moral free space" are various *hypernorms*, or "principles so fundamental that, by definition, they serve to evaluate lower order ethical norms. *Id.* at 44.

[179] *See* MARKLE FOUNDATION, *supra* note 9, at 6.

unwarranted manner. This includes a vow on the part of the websites to continuously update privacy-protection technology and applications in a commercially-reasonable fashion.

¶87 In the current landscape, the following are only some options to enhance the architecture of online health privacy:

- De-identifying and anonymizing information;
- Denying search engines access to cyber-patient information ;
- Facilitating online confidentiality agreements between cyber-patients;
- Granting cyber-patients the ability to register a list of banned visitors to their profiles;
- Issuing quarterly reports on the state of privacy on the website;
- Ensuring cyber-patients' ability to file complaints and appeals and resolve disputes with other users through trusted mechanisms; and
- Allowing users to export their stored information, including profiles and postings.

Ensuring ISPs put forth best efforts to update and maintain a level of privacy protection enables cyber-patients to better control their information, thereby preventing aggregation, identification, and dissemination to unwanted parties.

2. Right to Informed Consent

¶88 Cyber-patients have the right to be educated before disclosing personal information online. They must have access to information regarding the technological medium and its capabilities, the website's privacy policies, and who has access to cyber-patient records, postings, and online activities.

¶89 Websites and cyber-patients can ensure informed consent while minimizing irrational privacy-protective behavior in the following ways:

- Clear and accessible policies detailing the consequences of participation in plain English (and/or other applicable languages);
- Prominently-placed privacy policies and notices;
- Mandatory tutorials about the website's operations, applications, use, and foreseeable consequences arising from its use;
- Adherence to a uniform and standardized privacy policy for all health networking websites, thereby lessening a cyber-patient's switching costs and allowing him to better manage his expectations; and
- Implementing an "opt-in" system, in which the highest privacy setting is the default and cyber-patients are charged with the burden of opting out for more disclosure.

Education raises cyber-patients' awareness to the potential harms associated with use of the network and empowers them to make sound, informed decisions regarding their privacy. Research indicates that the mere mention of privacy concerns predisposes

individuals to be more cautious.[180] This heightened level of awareness will minimize over-exposure, confidentiality breaches, and unwanted dissemination of information.

3. Right to Control Disclosure of Information

¶90 Once informed, individuals are in the best position to decide what information to disclose and to whom. Cyber-patients must have the right to control their information. This includes the ability to grant or deny access to their information. Moreover, cyber-patients must have a right to determine what information is private on a context-by-context basis.

¶91 Websites and cyber-patients can better control the disclosure of digital information to unwanted audiences in the following ways:

- Allowing cyber-patients to set the specific levels of confidentiality expected of each post, information, or audience;
- Granting cyber-patients the ability to segregate audiences or "zone" profiles according to the nature of the relationship with the audience;
- Providing cyber-patients with the choice to opt-in to (rather than opt-out of) behavioral targeting;
- Enabling users to decide how the website uses their information, whether personally identifiable or not;
- Permitting cyber-patients to permanently disable a profile and delete its contents;
- Facilitating the execution of confidentiality agreements among users; and
- Providing the ability to tag information as private and create audit trails of user and ISP disclosure.

Providing cyber-patients the ability to disclose selective information to different audiences enables them to enjoy all the benefits of networking while reducing the risk of harms such as identification, aggregation, dissemination, and breach of confidentiality. It allows cyber-patients to be truthful without fearing self-exposure will have adverse consequences.

4. Right to Transparency

¶92 Cyber-patients must have the right to know exactly how their personal information is used, collected, and accessed. Further, they must know who else has access to it. This right encompasses the ability of the individual to inspect and modify their information and to obtain records of disclosures and authorizations.

---

[180] Brad Stone, *Our Paradoxical Attitudes Toward Privacy*, BITS: N. Y. TIMES TECHNOLOGY BLOG, July 2, 2008, http://bits.blogs.nytimes.com/2008/07/02/our-paradoxical-attitudes-towards-privacy/ (citing a study suggesting that "when the issue of confidentiality was raised, participants clammed up. For example, 25 percent of the students who were given a strong assurance of confidentiality admitted to having copied someone else's homework. Among those given no assurance of confidentiality, more than half admitted to it. The assurances, the researchers theorized, 'raise issues of privacy that might not otherwise figure prominently in people's minds.' In other words, the less people think about privacy (and sitting in an empty room staring at the computer, who does?), the more they lower their guard.").

¶93 Website operators and ISPs can strengthen the right to transparency in the following ways:

- Full disclosure of all uses of members' information, whether de-identified or not, including all possible commercial uses and sales;
- Clearly articulated website policies regarding compliance with civil subpoenas;
- Reasonable advance notice and opportunity to opt-out of any change to the website's terms of use or privacy policy before implementation;
- The ability to track disclosed information or documents deemed sensitive to establish a trail of accountability among users;
- Disclosure regarding any invisible audiences who have access to cyber-patient postings (employees of ISP, etc.);
- Optional alerts to consumers when behavioral tracking is being performed;
- A clear policy on the question of how long the website will keep cyber-patient information, postings, etc.; and
- A clear policy on searchability (i.e., whether search engines or the website allows searching for posts within the website).

Transparency ensures that users are notified of any access, use, or breach of their health information by the website or third parties. This knowledge empowers cyber-patients to act promptly by altering privacy settings or abandoning the website, thereby limiting harms such as information collection, aggregation, and invasion.

5. Right to Accessibility and Portability

¶94 Cyber-patients must have the right to access, alter, and delete any information pertaining to them. They must also have the right to easily transfer their profiles to another online health network.

¶95 The multiple parties involved can enable consumer choice and portability in the following ways:

- Granting the ability to export user profiles, much like the FCC has granted to wireless local telephone numbers with Local Number Portability, [181] enabling users to switch networks without affecting the integrity of their health information;
- Requiring service providers to keep the cyber-patient's postings for a reasonable period of time designated by the cyber-patient;
- Allowing cyber-patients access to any behavioral profile detailing their tracked online activities; and
- Allowing cyber-patients to alter or delete such behavioral tracking profiles.

Accessibility and portability minimize the risk of loss of health information stored on an online health profile. This right ensures control and retention of records for banished

[181] 47 C.F.R. §§ 52.23–33 (2008).

website users, former users of no longer existing websites, and users wishing to switch websites. This grants cyber-patients the liberty to leave a website that forces them to sacrifice certain privacy protections and increases their chances of becoming a victim of information collection, aggregation, identification, and dissemination.

6. Right to Due Process and Dispute Resolution

¶96 Cyber-patients must have the right to be notified of, defend, and appeal any allegation or charge of conduct that could result in their removal from the website or loss of information contained therein. Cyber-patients must also have access to a trusted forum for dispute resolution.

¶97 Due process and dispute resolution can be established in the following ways:

- Creating a trusted internal forum for the resolution of user-to-user disputes;[182]
- Participating in a trusted third party dispute resolution system;[183]
- Allowing users to flag or dispute false or harmful information posted by other users;
- Reasonable notice in advance of membership termination, along with the ability to export documents and information kept on the terminating network and the ability to alert fellow members of a cyber-patient's new "address";
- Ensuring the cyber-patient's right to know the reason of termination or expulsion from an online network; and
- Ensuring the cyber-patient's ability to defend and appeal a termination.

Due process presents cyber-patients with an extra level of protection from exclusion. Allowing users to address accusations of wrongdoing and contest network expulsions is imperative. A proper dispute resolution system could limit harms resulting from the unwanted disclosure of information, identification, breach of confidentiality, and invasion. The mere existence of a dispute resolution system would certainly act as a deterrent to privacy-offending behavior.

7. Right to Heightened Protection for Minors

¶98 Cyber-patients who are minors have a right to a heightened level of privacy protection on each of the foregoing enumerated rights. This right provides an additional shield of protection to a population especially vulnerable to the privacy harms of health networks. Minors are more likely to be the victims of online privacy harms due to their lacking full comprehension of the consequences of over-exposure online and overly-

[182] Some sites where a dispute can arise over the accuracy or objectivity of information can be questioned, such as Wikipedia, already provide internal dispute resolution modules for their users. *See* Wikipedia Dispute Resolution, http://en.wikipedia.org/wiki/Wikipedia:Dispute_resolution (last visited June 3, 2008).

[183] Outsourcing disputes among users to a third party dispute resolution company have already been seen in the world of e-commerce when eBay provided its users with the opportunity to solve their issues in a third party forum, SquareTrade. *See* SquareTrade ODR, http://www.squaretrade.com/pages/odr-discontinued (last visited June 3, 2008) (the ODR is now discontinued due to change in the eBay system).

optimistic nature regarding risk. Both ISPs and caretakers should be charged with the duty to safeguard minors.

¶99 The following recommendations could begin to ensure a proper level of protection for minors on health networking websites:

- Participation in a mandatory tutorial regarding privacy online, perhaps even as part of a school curriculum;
- Restriction of other users' ability to view a minor's profile;
- ISP vow to refrain from monitoring minors website visits, postings, etc.; and
- Age verification techniques.[184]

These safeguards shield minors from over-exposure, identification, dissemination, and information collection.[185]

8. Right to Anonymity

¶100 Cyber-patients must have the right to communicate anonymously, subject to certain limitations. By masking identity, cyber-patients can interact freely and confidently without fearing stigmatization.

¶101 The following tools should be implemented by ISPs to allow cyber-patients to post freely while respecting others:

- Providing clear language defining anonymity and educating users about the level of protection against identification on the website and how it is affected by altering privacy settings;
- Providing users with available technological tools to mask their identities in appropriate and clearly-defined circumstances (anonymization through technology);
- Assuring third parties will not gain access to identified information; and
- Indicating the precise circumstances (such as a government-issued subpoena) under which the ISP will provide a party with user information, whether content-related or otherwise.

The ability to maintain anonymity or pseudonymity are critical to a cyber-patient's free expression, but must be balanced against the rights of other cyber-patients to be free from

[184] Although online verification technology currently exists, it is neither consistently accurate nor popularly supported. Reno v. A.C.L.U., 521 U.S. 881, 881–82 (1997) (finding that it was not feasible for many website publishers to use age verification devices because of their expense and their imprecision in determining ages). *See* Catherine Crump, *Data Retention: Privacy, Anonymity, and Accountability Online*, 56 STAN. L. REV. 219 (2003) (arguing that government compelled identity disclosure would destroy all the current benefits that the Supreme Court recognized in *Talley v. California* and *McIntyre v. Ohio Elections Commission* that anonymity affords internet users such as the inhibited dissemination of true information that could be curtailed by the fear of reprisal).

[185] Although this heightened protection may prevent various privacy harms, it could also unreasonably restrict minors' freedom on the network. Frustrated by overburdening restrictions and denial to certain network features, minors may actively seek to conceal or change their age on the network, potentially increasing the likelihood of harm if others online were to believe he is of age.

harassment and fallacy. Anonymity minimizes the damages caused by identification, insecurity, and dissemination of information.

B. Responsibilities of Cyber-Patients

¶102 It is axiomatic that with every right comes a duty. Cyber-patients must be charged with responsibilities over their online privacy as follows.

1. Duty to Understand

¶103 Cyber-patients have a duty to understand the nature of the online setting and adjust expectations of privacy accordingly. Disclosure always involves risk. Armed with the rights of ISP transparency and informed consent, users must assume the following responsibilities:

- Seeking, reading, and understanding the website's terms and policies;
- Adjusting their behavior, expectations, and reliance on online health information accordingly;
- Establishing desired privacy settings; and
- Understanding the nature of the digital social forum.

Informed cyber-patients are more apt to act appropriately and avoid breaching other users' privacy, or even their own.

2. Duty to Maintain the Confidentiality of Fellow Users' Information

¶104 Cyber-patients have the duty of confidentiality to fellow patients. All information disclosed on health networking websites is privy and not to be divulged or otherwise disseminated. Users should not disclose any information obtained through the website unless specifically authorized. Similarly, disclosing cyber-patients should be as clear as possible regarding the level of confidentiality they expect. Cyber-patients have the duty to obtain the consent of family members and others whose health information they disclose. Relevant information regarding the health of family members is a vital part of a complete medical record. However, cyber-patients must understand these individuals also have rights to privacy in their health information. Cyber-patients must, therefore, obtain the informed consent of their family members before posting such information on the website.

¶105 Cyber-patients' responsibility to maintain the confidentiality of other users prevents various information dissemination harms.

3. Duty to Refrain from Using Network for Commercial or Other Illicit Purposes

¶106 Cyber-patients have the duty to refrain from using the health network illicitly. Commercial, political, and other hidden agendas can compromise the benefits of online health networks. Cyber-patients must restrict use of health networks to their intended and stated functions, and abstain from any activity deviating from the website's purpose.

¶107 Cyber-patients have the related duty to ensure good information on the network to the best of their abilities. Inaccurate health information can result in invasive physical,

emotional, or financial harm to fellow cyber-patients.[186] Cyber-patients should flag or question any posted information that they believe to be erroneous or misleading.

V. CONCLUSION

¶108 *Primum, non nocere*, or "first, do no harm,"[187] is a governing precept for physicians, reminding them to weigh the possible harms of a medical intervention against the probability of benefit to the patient. This ancient norm embodies the constitutional duty of the doctor to the patient. Similarly, modern healthcare laws such as HIPAA have created duties and rights among healthcare providers and consumers fundamentally based on their relationships and roles.

¶109 Online health networking has transformed the foundational relationships in health care by changing how, why, and to whom cyber-patients disseminate personal healthcare information. While social media applied to health care has many possible benefits relating to patient care, it currently exists in a legal and normative vacuum. This vacuum has serious implications for the privacy interests of cyber-patients and others whose information may be disclosed online, as they can neither rely on the ex ante protection of statutory law nor the redress of privacy tort law.

¶110 In the absence of law, actors in this new healthcare environment must embrace ethical norms designed to meet the challenges posed by the technologies in use. This Article proposes the Cyber-Patient's Bill of Rights and Responsibilities, a normative protocol for immediate consideration and application. It is only through the definition of expectations, rights, and duties that new health media technologies can aim to do no harm.

[186] Anthony G. Crocco et al., *Analysis of Cases of Harm Associated With Use of Health Information on the Internet*, 287 JAMA 2869 (2002) (arguing that the harm from online misinformation can be physical (e.g., due to inappropriate treatments, adverse effects, or untreated disease), emotional (e.g., from false hope or anxiety regarding unfounded diagnostic, prognostic, or therapeutic information), or financial (e.g., expenses associated with unnecessary second opinions and purchase of inappropriate services or products)).

[187] Origin unknown, but commonly attributed in error to the Hippocratic Oath. *See* Wikipedia, Primum Non Nocere, http://en.wikipedia.org/wiki/Primum_non_nocere (last visited July 22, 2008).