PERSONAL HEALTH INFORMATION SHARED VIA SOCIAL NETWORKING:

THE GAP BETWEEN REALITY AND PROTECTION[1]

Madison M. Pool

ABSTRACT

Control over personal information has long been valued in American society as a lynchpin of privacy. Traditional causes of action evolved to protect this privacy in a world confined by the bounds of physical space. However, these approaches fail to adequately remedy the harms confronted in the modern world of cyberspace. When Congress passed the Health Insurance Portability and Accountability Act of 1996, it recognized the revolutionary impact electronic medical records would have on individuals' control over their personal health information (PHI) in the health care context. This legislation not only laid the foundation for protection of PHI through the HIPAA Privacy Rule, it also statutorily validated this long-held American value of control over personal information in the form of protections for PHI. Although the HIPAA Privacy Rule established the first set of federal standards for protection of this highly valued category of information, it remains limited to a narrow group of covered entities.

Not only is PHI disclosed in social networking not protected by current federal regulations, it is also largely unprotected by state law. State law protections are still predominated by antiquated physical-space based causes of action that ignore the realities of social networking in a context unconstrained by geographic borders. Combined, the shortcomings of federal legislative protections and the outdated state protections result in a gap between the realities of social networking and the available protections for PHI. Social networking's ubiquity and the expectations of privacy held by users and promoted by the sites themselves challenge the values of privacy and protection for PHI. When the HIPAA Privacy Rule was established in 1996, Facebook did not exist. However, the legislation was envisioned as a floor on which to build protections as technology

1. I am grateful to Professor Ani Satz for her advice and mentorship on this project, and to Julia Hueckel, Bonnie Scott, and Francesca Pisano for their support and detailed comments on drafts. I would also like to thank Wes Floyd and Brett Snyder for sharing their expertise. Finally, I would like to thank Jeff Pool for his patience, input, and tireless support throughout this process.

and electronic storage of PHI evolved. Social networking is just such an evolution.

This Note proposes the adoption of federal regulations to protect PHI disclosed through online social networking. From rapidly and unpredictably changing privacy settings, to sale of information to advertisers, there are many ways in which PHI is disclosed and disseminated further than the user's known or intended audience. If protection for PHI does not keep pace with the development of online social networking, users will increasingly find themselves without meaningful remedies to address emerging harms.

INTRODUCTION

Tom is a social networking user.[2] He restricted his privacy settings so that only a small group of his "friends" could see his postings. These postings included a discussion of his struggles with diabetes. Without warning, the site changed its privacy settings and Tom's postings—including his diabetes dialogue—became visible to everyone who subscribes to the site and hundreds of millions of other users, including his boss. Not only were his postings visible, but his picture also began appearing on other users' pages next to advertisements for diabetes medications. In frustration, Tom attempted to delete his profile and erase all this information from the site. To his dismay, the site informed him that the information could not be deleted. Suddenly, the privacy settings Tom had been so vigilant in monitoring seemed like a sham.

While Tom is merely an illustrative example, the problems are real and mirror the experiences of millions of social networking users.[3]

---

2. This example is fictional and the name invented; any resemblance to a real person or story is coincidental. For a real life example, *see* Julia Angwin & Steve Stecklow, *"Scrapers' Dig Deep for Data on the Web,* WALL ST. J. (Oct. 11, 2010 9:30 PM), http://online.wsj.com/article/SB10001424052748703358504575544381288117888.html ("'I felt totally violated,' says Bilal Ahmed . . . who used PatientsLikeMe to connect with other people suffering from depression. He used a pseudonym on the message boards, but his PatientsLikeMe profile linked to his blog, which contains his real name.").

3. Facebook has more than one billion monthly active users, with 618 million active daily users as of December, 2012. *Key Facts*, FACEBOOK (Dec. 31, 2012), http://newsroom.fb.com/Key-Facts. As of September 8, 2011, Twitter reached 100 million active users. @Twitter, *One Hundred Million Voices*, TWITTER BLOG (Sept. 8, 2011, 9:32 AM), http://blog.twitter.com/2011/09/one-hundred-million-voices.html. [hereinafter @Twitter Voices]. Discontent with such practices has been discussed for several years. *See, e.g.*, *Facebook Reveals 'Simplified' Privacy Changes*, BBC (May 26, 2010),

With social networking on the rise,[4] issues of informational privacy are also increasing.[5] Yet despite social networking pitfalls, a fascinating phenomenon has arisen—users are increasing activity.[6] Social networking is becoming more ingrained and incorporated into everyday life: socially, politically, and even in the workplace.[7] Many users, like Tom, continue to believe their information is far more protected than it is. The reality of obtuse privacy policies, limited user control, and widespread distribution of personal information to third parties are obscured by the sites' promotions advertising privacy control and "sharing but like real life."[8] These implications of

http://www.bbc.co.uk/news/10167143 (praising increased privacy settings options but criticizing the disregard of personal data sales to advertisers); *see also* Kevin Bankston, *Facebook's New Privacy Changes: The Good, The Bad, and The Ugly*, ELEC. FRONTIER FOUND. (Dec. 9, 2009), https://www.eff.org/deeplinks/2009/12/facebooks-new-privacy-changes-good-bad-and-ugly (criticizing new Facebook privacy changes as "clearly intended to push Facebook users to publicly share *even more* information than before" and reducing user control over "personal data.") (emphasis in original). However, there had been no resolution until the recent settlement agreement with the Federal Trade Commission ("FTC"). *See* Emil Protalinski, *Facebook settles with FTC over default privacy settings*, ZDNET (Nov. 29, 2011, 10:09 AM), http://www.zdnet.com/blog/facebook/facebook-settles-with-ftc-over-default-privacy-settings/5667(discussing the settlement terms).

4. For example, Twitter reported an average of 460,000 new accounts created per day from mid-February, 2011, to mid-March, 2011 and a 182% increase in the number of mobile users from March 2010 to March 2011. @Twitter, *#numbers*, TWITTER BLOG (Mar. 14, 2011, 11:38 AM) http://blog.twitter.com/2011/03/numbers.html.

5. *See, e.g.*, Maria Aspan, *How Sticky Is Membership on Facebook? Just Try Breaking Free*, N.Y. TIMES (Feb. 11, 2008), http://www.nytimes.com/2008/02/11/technology/11facebook.html?pagewanted=all (discussing difficulties with permanently deleting information from Facebook); *see also* Alex Pell, *Hey, Facebook, Just Let Go of Me*, SUNDAY TIMES (Mar. 16, 2008), http://technology.timesonline.co.uk/tol/news/tech_and_web/the_web/article3553216.ece (discussing lack of control of personal information resulting from the option to "deactivate," but not permanently delete, a Facebook profile).

6. *See, e.g.*, *Tweet, tweet! Using Twitter to Build Career Connections Now*, STUDENT LAW., Sept. 2011, at 8; Joe Dysart, *Viral Information: Interactive press releases really spread the word*, ABA J, Oct. 2011, at 32; @Twitter Voices, *supra* note 3.

7. *See, e.g.*, @Twitter Voices, *supra* note 3; *Tweet, tweet! Using Twitter to Build Career Connections Now, supra* note 6, at 8; Dysart, *supra* note 6, at 32.

8. Google, *Google+: Sharing but like real life*, YOUTUBE (Nov. 23, 2011), http://www.youtube.com/watch?v=GRmDGvdkg8E ("Sharing but like real life." quote appears at time code 1:21).

privacy, which mask the sites' actual practices, undermine users' legitimate privacy expectations.[9] Disturbingly, current law does not adequately protect social networking users.[10]

One area in which this lack of protection is particularly worrisome is personal health information, which Americans attach great importance to protecting.[11] Americans value protecting privacy through control of personal information generally,[12] but PHI has received extra attention over the past two decades.[13] Control over personal information is particularly pertinent to PHI because of its uniquely high potential for misuse, embarrassment, pain, and discrimination.[14] However, protection for PHI is largely lacking in social networking. With the continued increase in social networking and the lack of protection under current law, a gap has resulted between social networking realities and PHI protections.

Current protection for PHI falls into two categories: federal regulatory protection and state protection.[15] Both of these categories fall short of preserving the control over PHI that American society expects.[16] First, current federal regulations are limited only to "covered entities"[17] and do not apply to social networking. Second,

9. *See infra* Part III.A.

10. *See infra* Part II.

11. Health and Human Serv. ("HHS") Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82,462, 82,464 (Dec. 28, 2000) (codified at 45 C.F.R. pts. 160 & 164) [hereinafter "2000 Privacy Standards]" ("Among different sorts of personal information, health information is among the most sensitive.").

12. *Id.* ("A right to privacy in personal information has historically found expression in American law.").

13. *Id.* ("Among different sorts of personal information, health information is among the most sensitive."). While much has been written about privacy issues with the advent of electronic medical records, other potential disclosures of personal health information have yet to be addressed. For example, both Nick Terry (Hall Render Professor of Law and Co-director of the William S. and Christine S. Hall Center for Law and Health at Indiana University Robert H. McKinney School of Law) and Sharona Hoffman (Professor of Law and Bioethics and Co-Director of the Law-Medicine Center at Case Western Reserve University School of Law) have written prolifically on this issue. *See infra* notes 24 and 101.

14. 2000 Privacy Standards, *supra* note 11, at 82,464 ("Among different sorts of personal information, health information is among the most sensitive.").

15. *See infra* Part II.

16. *See infra* Part II.

17. 2000 Privacy Standards, *supra* note 11, at 82,476–77 (defining covered entities as "health plans, health care clearinghouses, and health care providers").

state protections fail for two reasons: the differing protection among states does not align with the reality that social networking is largely unrestricted by state and even national borders,[18] and traditional causes of action apply imperfectly, if at all, to privacy needs in an online social networking setting.[19] These causes of action are characterized by a focus on physical space and retrospective rather than preventative measures, neither of which comport with the realities of harms in online social networking.[20]

This Note addresses the novel issue of protection for PHI in social networking[21] and proposes the adoption of federal regulations to keep pace with online social networking's rapid evolution and provide protection for PHI disclosed in this setting. Part I of this Note highlights the value Americans place on preserving informational privacy by controlling personal information. Privacy is a value strongly embedded both in American legal history[22] and in American cultural understanding,[23] and PHI is one area in which value of

18. *See, e.g.*, Proto v. Hamic, No. FSTCV106005537S, 2011 WL 1992202 (Conn. Super. Ct. May 10, 2011) (Connecticut resident brought claim against former student now residing in Texas; court found jurisdiction under Connecticut long-arm statute). In addition, Facebook reports that "approximately 80% of [its] monthly active users are outside the United States and Canada." *Fact Sheet*, FACEBOOK (Feb. 19, 2012), http://newsroom.fb.com/content/default.aspx?NewsAreaId=22.

19. *See, e.g.*, Patricia Sanchez Abril, *A My(Space) of One's Own: On Privacy and Online Social Networks*, 6 NW. J. TECH. & INTELL. PROP. 73 (2007–08); Lior Jacob Strahilevitz, *Reunifying Privacy Law*, 98 CAL. L. REV. 2007 (2010); Spencer D. Kiggins, *Privacy in Health Information Technology in the Age of Electronic Informational Piracy*, 10 TELEHEALTH L.J. 33 (2009).

20. *Cf.* Romano v. Steelcase Inc., 907 N.Y.S. 650, 655, n.6 (N.Y. Sup. Ct. 2010) (citing Cordero v. NYP Holdings, Inc., 866 N.Y.S.2d 90 (Sup. Ct. NY Co. 2008) (finding no common law right of privacy in New York)) and Fraley v. Facebook, Inc., 830 F. Supp. 2d 785, 803 (N.D. Cal. 2011) (finding use of plaintiff's profile pictures and names sufficient to state a claim under "long recognized a right to protect one's name and likeness against appropriation by others").

21. For example, MCGRADY ON SOCIAL MEDIA makes only one mention of HIPAA ("legislated privacy rights are derived from several federal and state laws . . . including . . . HIPAA"). PAUL D. MCGRADY, JR., MCGRADY ON SOCIAL MEDIA § 5.03 (also making no mention of personal health information).

22. *See, e.g.*, Griswold v. Connecticut, 381 U.S. 479, 483 (1965); 2000 Privacy Standards, *supra* note 11 at 82,464 (There are "enduring values in American law that relate to privacy," including a common law or statutory right to privacy recognized in every state, and "[m]any of the most basic protections in the Constitution.").

23. 2000 Privacy Standards, *supra* note 11 at 82,464.

control over personal information is particularly evident.[24] The belief that PHI should be afforded privacy protection has been statutorily validated by the enactment of the Health Insurance Portability and Accountability Act of 1996 and the Health Information Technology for Economic and Clinical Health Act.[25] This Part will discuss the values that underlie the passage of these two Acts to show the importance American society places on protecting PHI.

Part II explores the shortcomings of current privacy protections for PHI shared via social networking. It will discuss the protections offered by current regulations and show how this protection is limited only to narrow categories of actors in the health care field, falling short of the necessary protection for PHI in social networking. This Part will also show that state protections are insufficient for two reasons. First, this Part will demonstrate how having differing causes of action across states does not align with the reality that social networking is largely unrestricted by state and even national borders. Second, it will discuss the failings of the available causes of action—specifically, their antiquated bases in physical space and failure to provide meaningful remedies through adherence to retroactive privacy protections.

Part III of this Note discusses the modern trend of social networking and suggests that this is a viable area in which to extend protections. This Part will show the value of protecting PHI disclosed in social networking settings by addressing four realities of social networking: (1) social networking is on the rise; (2) social networking is valuable; (3) users expect that they will have control over their information; and (4) this expectation of privacy is undermined by the sites' conflicting privacy representations. This Part will further show the value of extending protections into this area by highlighting harms that will result to social networking users if the disconnect between expected and actual protections remain unaddressed. These harms include an inability to delete personal information after it is posted, disclosure beyond the intended audience through unexpected

24. *See, e.g.*, Daniel J. Gilman & James C. Cooper, *There is a Time to Keep Silent and a Time to Speak, the Hard Part is Knowing Which is Which: Striking the Balance Between Privacy Protection and the Flow of Health Care Information*, 16 MICH. TELECOMM. & TECH. L. REV. 279, 284 (2009–10); *see also* Sharona Hoffman & Andy Podgurski, *In Sickness, Health, and Cyberspace: Protecting the Security of Electronic Private Health Information*, 48 B.C. L. REV. 331, 335-36 (2007).

25. *See* Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (1996) [hereinafter HIPAA; HIPAA Privacy Rule, 45 C.F.R. §§ 160 & 164 (2010) [hereinafter HIPAA Privacy Rule]; and Health Information Technology for Economic and Clinical Health Act, Pub. L. No. 111-5, Title XIII, Div. A & Title IV, Div. B (2009) [hereinafter HITECH] (part of the American Recovery and Reinvestment Act of 2009).

and non-optional privacy changes, and the sale of personal information to third party sites.

Part IV will advance a proposal for federal regulations to remedy the shortcomings of the current law. The proposed regulations would address the gap in the law in three ways. First, the regulations would require meaningful privacy disclosures and truthful advertising by the social networking sites. Second, the regulations would establish guidelines for PHI use and distribution by social networking sites and third-party affiliates. Third, the regulations would provide meaningful causes of action and remedies for users and sites alike. This Part will also discuss the advantages of such a federal regulatory scheme, including filling the current gap in the law, providing meaningful dispute resolution options and remedies, and setting clear expectations for all parties involved.

Finally, Part V further outlines the beneficial ramifications of such a solution.[26] With the rapid advancements in social networking, data management, and patient-managed electronic medical records, such regulations could serve as a benchmark for mitigating other harms before they arise.

I. CONTROL OF PERSONAL HEALTH INFORMATION: A MODERN RECOGNITION OF HISTORICAL AMERICAN PRIVACY VALUES

Privacy is a value strongly embedded both in American legal history[27] and in American cultural understanding; "it speaks to . . . individual and collective freedom."[28] From informational privacy to physical privacy, "the rights of the individual" have been at the "forefront of [American] democracy."[29] One way these rights are respected is through a privacy-based theory of control.[30] Privacy through control can apply both to controlling one's physical space and to controlling access to one's personal information.[31] The right to

26. While this Note focuses on PHI disclosed in a social networking setting, the proposed regulatory scheme could be adapted to fit other categories of information and other data-mining settings.

27. *See supra* note 22 and accompanying text.

28. 2000 Privacy Standards, *supra* note 11, at 82,464.

29. *Id.*

30. *See, e.g.*, Avner Levin & Patricia Sanchez Abril, *Two Notions of Privacy Online*, 11 VAND. J. ENT. & TECH. L. 1001 (2008–09); Patricia Sanchez Abril, *Private Ordering: A Contractual Approach to Online Interpersonal Privacy*, 45 WAKE FOREST L. REV. 689 (2010); Patricia Sanchez Abril, *Recasting Privacy Torts in a Spaceless World*, 21 HARV. J. L. & TECH. 1 (2007–08).

31. *See* Levin & Abril, *supra* note 30, at 1007-08 (discussing ways of thinking about the concept of "privacy"). This Note focuses on

privacy through control of personal information "has historically found expression in American law."[32] This tradition continued with the passage of the Health Insurance Portability and Accountability Act of 1996 (HIPAA).[33]

As a nation, the United States places high value on protecting PHI.[34] PHI includes "information . . . that . . . relates to the past, present, or future physical or mental health or condition of an individual."[35] This information is extremely personal and intimate, and its disclosure has a uniquely high potential for misuse, embarrassment, pain, and discrimination.[36] Statutes passed over the last two decades have provided PHI with privacy protection.[37] Congress passed HIPAA in part to establish "standards with respect to the privacy of individually identifiable health information."[38]

In passing HIPAA, "Congress recognized the importance of protecting the privacy of health information given the rapid evolution of health information systems."[39] Pursuant to this goal, the U.S. Department of Health and Human Service (HHS) promulgated final rules and regulations to establish such standards.[40] Published on August 14, 2002, the regulations are now known as the HIPAA

---

informational privacy exercised via control over access to one's personal information.

32. 2000 Privacy Standards, *supra* note 11, at 82,464.

33. HIPAA, *supra* note 25.

34. *See supra* notes 23 and 24.

35. HIPAA Privacy Rule, *supra* note 25, at § 160.103.

36. *See* 2000 Privacy Standards, *supra* note 11, at 82,464 ("Among different sorts of personal information, health information is among the most sensitive.").

37. *See generally* HIPAA, *supra* note 25A; HIPAA Privacy Rule, *supra* note 25; and HITECH, *supra* note 25.

38. HIPAA, *supra* note 25, at § 264(a–b) ("The recommendations under subsection (a) shall address at least the following: (1) The rights that an individual who is a subject of individually identifiable health information should have. (2) The procedures that should be established for the exercise of such rights. (3) The uses and disclosures of such information that should be authorized or required."). Individually identifiable health information is health information "[t]hat identifies the individual; or . . . [w]ith respect to which there is a reasonable basis to believe the information can be used to identify the individual." HIPAA Privacy Rule, *supra* note 25, at § 160.103.

39. HHS Standards for Privacy of Individually Identifiable Health Information, 67 Fed. Reg. 53,182 (Aug. 14, 2002) (codified at 45 C.F.R. pts. 160 & 164) [hereinafter Privacy Standards Modifications].

40. *Id.* at § 264(c); HIPAA Privacy Rule, *supra* note 25.

Privacy Rule[41] and "create[d], for the first time, a floor of national protections for the privacy of [individuals'] most sensitive information—health information."[42]

One of the HIPAA Privacy Rule's foremost purposes is "[t]o protect and enhance the rights of consumers by providing them access to their health information and controlling the inappropriate use of that information."[43] HHS recognized the area had a pressing need for informational protection when it promulgated the regulations.[44] The HIPAA Privacy Rule sets out comprehensive requirements regarding the use and disclosure of protected health information.[45] To reiterate that the HIPAA Privacy Rule is a minimum standard, HHS added that it "creates a framework of protection that can be strengthened by both the federal government and by states as health information systems continue to evolve."[46]

In explaining the need for the HIPAA Privacy Rule, HHS noted that "few experiences are as fundamental to liberty and autonomy as maintaining control over when, how, to whom, and where you disclose personal material."[47] The HIPAA Privacy Rule is a landmark regulation that created the first set of federal standards for protection of PHI,[48] and it recognizes the importance of protecting this category of information.[49]

---

41. HHS issued the Privacy Rule to implement requirements of the Health Insurance Portability and Accountability Act of 1996. *See* U.S. Dept. of HHSS, Office for Civil Rights, *Summary of the HIPAA Privacy Rule*, 1 (2003), http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/privacysummary.pdf. [hereinafter PRIVACY RULE SUMMARY] (A slight misnomer: the HIPAA "Privacy" Rule provides standards for "individuals' privacy rights to understand and control how their health information is used" that in operation preserve the right of informational control and confidentiality rather than strict privacy.).

42. Privacy Standards Modifications, *supra* note 38.

43. 2000 Privacy Standards, *supra* note 11, at 82,463.

44. 2000 Privacy Standards, *supra* note 11, at 82,462 ("These protections will begin to address growing public concerns that advances in electronic technology and evolution in the health care industry are resulting, or may result, in a substantial erosion of the privacy surrounding individually identifiable health information. . . .").

45. *Id.*

46. 2000 Privacy Standards, *supra* note 11, at 82,464.

47. *Id.*

48. *Id.*; *see also* PRIVACY RULE SUMMARY, *supra* note 41 at 1.

49. 2000 Privacy Standards, *supra* note 11 at 82,463 ("In enacting HIPAA, Congress recognized the fact that administrative simplification cannot succeed if we do not also protect the privacy and confidentiality of personal health information."); *see also*, PRIVACY RULE SUMMARY, *supra* note 41, at 1 (balancing an assurance of proper protection for

The HIPAA Privacy Rule's framework was expanded with the passage of the Health Information Technology for Economic and Clinical Health (HITECH) Act, providing more protection for health information maintained electronically.[50] Individuals now have the statutory right to know who has accessed their health information, a response to the pitfalls of electronically maintaining medical records.[51] The requirement illustrates the value placed on privacy protection for electronic, sensitive information,[52] as HHS recognized a fundamental right to privacy embodied in PHI.[53]

However, despite PHI's sensitive nature, the current regulatory protections are limited. They do not extend beyond a few narrow classes of "covered entities,"[54] and do not address the social networking issues. Additionally, state laws do not offer adequate protection for PHI shared in social networking interactions, with provisions that "vary significantly from state to state" often failing to provide basic protections.[55] These shortcomings were the reason for developing federal regulations to safeguard PHI in the first place.[56] As noted by HHS, "Privacy is a fundamental right. As such, it must be viewed differently than any ordinary economic good."[57] The privileges and stringent privacy requirements established under these regulations are in place even though covered entities and their business associates are providing valuable services to individuals.[58]

---

individuals' health information while permitting "important uses" of that information is a "major goal" of the Privacy Rule).

50. HITECH Act, 123 Stat. 230, P.L. 115-5 (codified as amended 42 U.S.C. 300jj-11) ("National Coordinator shall perform the duties under subsection (c) in a manner consistent with the development of a nationwide health information technology infrastructure that allows for the electronic use and exchange of information").

51. 123 Stat. 230, P.L. 115-5, §13405(c)(1)(B) (codified as amended 42 U.S.C. 17935) ("[A]n individual shall have a right to receive an accounting of disclosures. . .").

52. *Id.*

53. 2000 Privacy Standards, *supra* note 11, at 82,464. ("Privacy is a fundamental right.").

54. *Id.* at 82,476–77 (These covered entities are "health plans, health care clearinghouses, and certain health care providers. . . .").

55. *Id.* at 82,463–64 (including access to a user's own medical records).

56. Privacy Standards Modifications, *supra* note 40, at 53,182. ("[H]ealth privacy protections are intended to provide consumers with similar assurances that their health information, including genetic information, will be properly protected.").

57. 2000 Privacy Standards, *supra* note 11 at 82,464.

58. *See generally* Strahilevitz, *supra* note 19; Kiggins, *supra* note 19; and Gilman & Cooper, *supra* note 24.

These requirements highlight the collective belief that individuals' PHI deserves strong protection.[59]

II. CURRENT PROTECTIONS FOR PERSONAL HEALTH INFORMATION ARE INSUFFICIENT

Despite the sensitivity of PHI and the belief that it should be protected,[60] current protections are limited.[61] Both the current federal regulatory protections and state protections fall short of providing adequate control over this valuable information.[62] Combined with social networking's rapid evolution, a significant gap has resulted between users' expected and actual control over PHI shared online.[63]

A. Federal Regulations: The HIPAA Privacy Rule and the HITECH Act

The first category of protection for PHI is federal: HIPAA and the HITECH Act.[64]

Despite the high value American society places on protecting the privacy of PHI, these protections are limited. As currently written, these standards only apply to certain "covered entities"[65] and their "business associates."[66] "Covered entities" are limited to health plans, health care clearinghouses, and certain health care providers.[67] The HIPAA Privacy Rule also applies these privacy requirements to the "business associates"[68] of covered entities.[69] However, they do not

59. *See generally supra* note 66 & 67.

60. *See supra* Part I.

61. *See supra* Part I.

62. *See supra* Part I.

63. *See* Privacy Standards Modifications, *supra* note 40, at 53,182 (noting consumer's concerns about the privacy of their personal information). *See also* 2000 Privacy Standards, *supra* note 11, at 82,462 (discussing how advances in technology affect individually identifiable health information).

64. *See supra* Part I.

65. 2000 Privacy Standards, *supra* note 11, at 82,476–77 (These covered entities are "health plans, health care clearinghouses, and certain health care providers. . . .").

66. HIPAA Privacy Rule, *supra* note 25, at § 164.502(e) (allowing a covered entity to disclose PHI to a business associate contingent upon "satisfactory assurance that the business associate will appropriately safeguard the information").

67. *Id.* at § 160.103.

68. *Id.* (defining business associate as "a person who: (i) On behalf of such covered entity . . . other than in the capacity of a member of the workforce of such covered entity . . . performs, or assists in the

provide protection outside of these narrow categories, thus failing to adequately protect PHI from disclosure in other settings.[70]

While the HIPAA Privacy Rule and the HITECH Act are steps in the right direction of establishing federal standards for privacy protection of PHI, they fall short of protecting PHI and privacy in the social networking setting. When HHS promulgated the HIPAA Privacy Rule, it noted consumers' increasing concerns "about the privacy of their personal information,"[71] specifically as "advances in electronic technology . . . are resulting, or may result, in a substantial erosion of the privacy surrounding individually identifiable health information. . . ."[72] HHS envisioned the HIPAA Privacy Rule as a floor that could be built upon as new technologies developed and offered challenges to protecting PHI.[73] Building on this floor with new federal regulations to protect PHI disclosed in social networking is a natural progression in addressing the increasing role played by social networking in our society.[74]

B. State Protections: Traditional Causes of Action

Because there are no federal regulations that directly protect PHI outside of the narrow parameters described,[75] most allegations of inappropriate use or disclosure of PHI in a social networking context are addressed by state law.[76] Protection for PHI varies across the

---

performance of: (A) A function or activity involving the use or disclosure of individually identifiable health information, including claims processing or administration. . . .").

69. *Id.* Generally, authorizations are required before protected health information may be disclosed by covered entities. *See id.* at §§ 164.502(a), 164.508(a).

70. *See, e.g.*, Hoffman & Podgurski, *supra* note 24 (discussing inadequate government response to protecting PHI).

71. Privacy Standards Modifications, *supra* note 40, at 53,182 (noting that the Privacy Rule creates a basic level of national protections to address public concern over privacy of their personal information).

72. 2000 Privacy Standards, *supra* note 11, at 82,462.

73. Privacy Standards Modifications, *supra* note 40, at 53,182 ("[T]he Privacy Rule creates, for the first time, a floor of national protections for the privacy of [consumers'] most sensitive information—health information.").

74. *See* Levin & Abril, *supra* note 30, at 1004 (discussing the reasonableness of the general public's expectation of privacy over their personal online information and their use of social networking sites to disclose personal information).

75. *See supra* Part II.A.

76. *See generally* Abril, *supra* note 19, at 78 (discussing state tort law as recourse for those wronged from disclosure of personal information via social networking); *see also* Nicholas P. Terry, *Physicians and Patients*

states and typically neither fully covers issues that arise in health care systems nor reaches other potential abuses of PHI.[77] Traditional common law causes of action are the most prevalent way plaintiffs petition courts for redress, and these causes of action have developed on a state-by-state basis.[78] However, this paradigm neglects important realities for addressing harms that occur in online social networking.

These traditional causes of action fail to provide protection for PHI disclosed in social networking in two ways. First, traditional causes of action vary by state largely ignoring the reality that social networking is largely unrestricted by state and even national borders.[79] Second, traditional causes of action apply imperfectly, if at all, to privacy needs in an online social networking setting because of: (1) outdated restrictions based on control of physical space, and (2) sole retrospective addressing of harms.[80]

1. *Differing Protections Across the States: Adherence to State Borders*

The lack of federal guidelines for privacy protection has resulted in a fragmented system across the states.[81] In discussing the importance of privacy for PHI, HHS noted that "[r]ules requiring the protection of health privacy . . . have been enacted primarily by the states . . . [and] vary significantly from state to state and typically apply to only part of the health care system."[82] HHS also noted that many of these state laws "fail to provide such basic protections as ensuring a patient's legal right to see a copy of his medical record."[83] Congress determined that privacy protection for PHI was sufficiently important to enact the first set of federal privacy protections for PHI.[84] Fragmented protection for health records was not acceptable;

Who "Friend" or "Tweet": Constructing a Legal Framework for Social Networking in a Highly Regulated Domain, 43 IND. L. REV. 285 (2010).

77. 2000 Privacy Standards, *supra* note 11, at 82,463 (noting wide variation in state law protection for health information).

78. *See* Abril, *supra* note 19, at 78; *see also* Terry, *supra* note 76.

79. *See, e.g.*, *Proto*, *supra* note 18; *see also Fact Sheet*, *supra* note 18.

80. *See* sources cited *supra* note 19.

81. 2000 Privacy Standards, *supra* note 11, at 82,463; *see also* Strahilevitz, *supra* note 19 (discussing the need for a re-examination and re-unification of privacy law generally to better accomplish the purpose of privacy torts); RESTATEMENT (SECOND) OF CONFLICT OF LAWS § 153 (1971) (noting that privacy rights are usually determined by law of the state where the plaintiff was domiciled if the matter complained of was published in that state).

82. 2000 Privacy Standards, *supra* note 11, at 82,463.

83. *Id.* at 82,464.

84. *Id.* at 82,463 (outlining the purposes underlying congressional enactment of the 2000 Privacy Standards).

similarly, fragmented protection for PHI shared in social networking should also be unacceptable. These protections, which are not nationally consistent, do not align with the reality that social networking is largely unrestricted by state and national borders.[85]

The need for protection of PHI in social networking is not limited to a particular state, as these issues regularly traverse state borders.[86] Consider, for example, *Proto v. Hamic*, [87] a Connecticut case in which a martial arts instructor brought an action against a former student who had moved to Texas.[88] The instructor alleged that the student, while residing in Texas, posted unfavorable content about him on the student's Facebook and Twitter accounts.[89] The court found personal jurisdiction under Connecticut's long-arm statute, holding that because the student knew the teacher was a Connecticut resident, and because the social networking postings could result in a harm to the teacher in Connecticut, the long-arm provision for committing "a tortious act within the state" was satisfied.[90] When discussing online issues, state lines cease to carry the same weight as in the non-cyber world.[91]

Despite social networking's ability to transcended geographic borders, protections for users are still affected by geography, even within states. One example illustrative of this artificial division is California users' inability to determine what uses of their likenesses or posted information are permissible. Compare, for example, *Cohen v. Facebook*[92] with *Fraley v. Facebook*.[93] Both cases arose in the Northern District of California, but in different divisions: *Cohen* in the San Francisco division and *Fraley* in the San Jose division.[94] Interestingly, even this small geographic distinction resulted in

85. *See supra* note 19

86. *See supra* note 19.

87. *See Proto*, *supra* note 18, at *1.

88. *Id.*

89. *Id.* at *1-2 ("[T]he plaintiff alleges that the defendant 'has designed and orchestrated an extensive campaign, using the Internet, to disseminate false, misleading, and disparaging information about [the plaintiff], and [the plaintiff]'s businesses, for the purpose of damaging [the plaintiff]'s professional reputation, driving away [the plaintiff]'s clients and affiliates, and gaining an unfair competitive advantage.'") (citation omitted).

90. *Id.* at *10-26.

91. *See supra* note 19.

92. Cohen v. Facebook, Inc., No. C 10-5282 RS, 2011 WL 5117164 (N.D. Cal. Oct. 27, 2011).

93. Fraley v. Facebook, Inc., 830 F.Supp.2d 785 (N.D. Cal. 2011).

94. *Cohen*, 2011 WL 5117164; *Fraley*, 830 F.Supp.2d 785.

differing outcomes. Both cases concerned the use of Facebook users' profile pictures for promotion of a new Facebook function.

In *Cohen*, users' names and pictures were distributed to others through a "Friend Finder" function designed to attract new users by linking current users to other people who they might know.[95] Gaining additional users resulted in more advertising revenue for Facebook[96] Ultimately, the court dismissed the plaintiffs' claims for misappropriation of their likenesses and unfair enrichment.[97]

In *Fraley*, users' names and profile pictures were paired with products and companies they had "liked," which were then displayed to the users' friends.[98] In contrast to *Cohen*, the *Fraley* plaintiffs' claims of misappropriation and unjust enrichment were allowed to move forward.[99]

The two claims were notably similar: both alleged Facebook had misappropriated the users' likenesses and unjustly benefitted from that use.[100] Both also took issue with Facebook's conduct because of the ultimate economic advantage to Facebook.[101] Yet, the cases were inconsistently resolved.[102] Cases like these underscore the difficulty for individuals and social networking sites alike to know what is an appropriate use of personal information under the current legal framework.

2. *Imperfect Application: The Limits of Physical Space and Retrospective Causes of Action*

The traditional causes of action available to plaintiffs are ill-fitted to this virtual world. Causes of action such as intrusion upon seclusion and defamation are often used in attempts to address wrongs arising from inappropriate disclosure of personal information online.[103] Scholars have observed that these traditional causes of action apply imperfectly, if at all, to privacy needs in an online social networking setting.[104] Two primary shortcomings highlight this imperfect fit. First, these traditional causes of action focus on privacy

95. *Cohen*, 2011 WL 5117164, at *2.

96. *Id.*

97. *Id.* at *3.

98. *Fraley*, 830 F.Supp.2d at 797.

99. *Id.* at 815.

100. *Cohen*, 2011 WL 5117164, at *1; *Fraley*, 830 F. Supp. 2d at 790.

101. *Cohen*, 2011 WL 5117164, at *1; *Fraley*, 830 F. Supp. 2d at 790.

102. *Cohen*, 2011 WL 5117164, at *1; *Fraley*, 830 F. Supp. 2d at 790.

103. *See* Abril, *supra* note 19, at 78-80 (discussing traditional torts and their potential application in the online realm).

104. *See supra* notes 19-20.

with regard to physical space,[105] which is largely incompatible with an online setting. Second, these causes of action are retrospective rather than preventative.[106]

First, the focus on physical space does not comport with the online medium. Traditionally, privacy has focused on control of physical space.[107] Privacy could be attained through an individual's ability to control access to his physical space or to control the distribution of information about himself within that space.[108] The tort of Intrusion upon Seclusion epitomizes the traditional focus on physical space in privacy protection. An actor is liable for invasion of privacy when he "intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns . . . if the intrusion would be highly offensive to a reasonable person."[109] While the definition provides that the intrusion could be a physical intrusion or "otherwise," courts have not expanded this concept beyond its traditional basis in physical space.[110]

This physical space framework is a poor fit for social networking. Online social networking is conducted in cyberspace; a virtual world that does not fit within the physical bounds that this cause of action envisions.[111] In addition, social networking is predicated on sharing information,[112] which is antithetical to seclusion.[113] Social networking

105. *See* Abril, *supra* note 19, at 79-80 (discussing how a plaintiff would need a reasonable expectation of privacy in a physical area to bring an action under traditional tort laws); *see also* RESTATEMENT (SECOND) OF TORTS § 652 (1977).

106. *See, e.g.*, RESTATEMENT (SECOND) OF TORTS § 559 (1977) (defining "defamatory communication" and discussing how the communication must have actually been made).

107. *See supra* notes 19-20.

108. *See, e.g.,* Abril, *supra* note 19 at 79 (discussing expectations of privacy in traditional tort law).

109. RESTATEMENT (SECOND) OF TORTS § 652B (1977).

110. This is evidenced by a LexisNexis search, returning only 21 results from a search of federal and state cases combined with the terms *intrusion w/2 seclusion AND ("social network" OR Facebook OR Twitter OR Google)*. Of these results, only one case is relevant: Maremont v. Susan Fredman Design Group, Ltd., No. 10 C 7811, 2011 U.S. Dist. LEXIS 140446, *21 (N.D. Ill. Dec. 7, 2011), (dismissing claim for intrusion upon seclusion on basis of information shared on Facebook and Twitter being "not private").

111. *Fact Sheet*, *supra* note 18 (detailing Facebook's online operation model).

112. *Fact Sheet*, FACEBOOK (Oct. 9, 2011, 3:14 PM), http://www.facebook.com/press/info.php?factsheet (Facebook's self-identified purpose is to "facilitate the sharing of information through the social graph, the digital mapping of people's real-world social connections. Anyone can sign up for Facebook and interact with the people they know in a trusted environment.").

is a rapidly evolving area that implicates PHI protections.[114] Traditional causes of action based in concepts of physical space fail to protect this highly valued category of information.[115]

The second reason these traditional causes of action apply imperfectly to social networking is that they are retrospective privacy protections. Adherence to retrospective measures ignores the reality that they provide little actual remedy for harms based on disclosure of information online. The traditional common law causes of action fall short because they are retrospective, thus, providing protection only in the form of causes of action arising after privacy is invaded.[116]

Defamation provides an example of retrospective protection.[117] A suit for defamation is a poor response to the actual harm that results when such statements are posted online. As illustrated in in *Proto v. Hamic*.[118] the defendant posted many negative remarks about his former teacher on Facebook and Twitter.[119] Information posted online can have a disturbing permanence.[120] Not only do sites limit users' abilities to delete information,[121] but it may also be impossible to trace where the information has spread.[122] Even if the teacher prevailed and the student removed the posting, the comments could have already spread beyond that site and may cause continual damage to the teacher's reputation.

---

113. *Id.*

114. *See infra* Part III.

115. There has been an increased emphasis on moving away from "physical-space-based" privacy torts to better reflect the reality of privacy in the social networking arena. *See, e.g.*, Abril, *supra* note 19; Kiggins, supra note 19; and Terry, *supra* note 76.

116. *See* RESTATEMENT (SECOND) OF TORTS § 559 (1977) (examples include defamation, intentional infliction of emotional distress, and false light privacy).

117. *Id.* ("A communication is defamatory if it tends so to harm the reputation of another as to lower him in the estimation of the community or to deter third persons from associating or dealing with him.").

118. *See supra* Part II.B.1; *Proto*, *supra* note 18, at *1-2.

119. *Proto*, *supra* note 18, at *1-2

120. *See supra* note 5,

121. *Id.*

122. Georgina Prodhan, *Analysis: New EU Data Laws Command the Tide But Not the Cost*, REUTERS (Jan. 24, 2012, 1:02 PM), http://www.reuters.com/article/2012/01/24/us-europe-data-legislation-idUSTRE80M1VL20120124 (discussing likely difficulty of enforcement of new E.U. data-protection proposals due in part to inability to trace and totally remove contested information).

Retrospective causes of action provide little if any protection before the inflicted harm in the social networking context. Despite a potential deterrent effect, these causes of action do not effectively respond once information has been posted, nor do they prevent all postings. There is relatively little case law on the subject,[123] which results in a lack of guidance for users and sites alike. With the potential for unwanted and unwarranted disclosure of information that brings with it an inability to delete the data,[124] PHI protection becomes a paramount concern. The spread of information as personal and valued as health information can cause particular harm.[125] If PHI is disclosed beyond its intended audience, the harm could include embarrassment, damage to relationships, and the impugning of reputations—the kinds of wrongs not easily remedied, if at all, and even less so in retrospect.[126] Once harmful information is disclosed online, it is difficult to trace its spread, and nearly impossible to remove.[127] To wait until the damage is done may result in no remedy at all.

III. PERSONAL HEALTH INFORMATION SHARED THROUGH SOCIAL NETWORKING DESERVES PROTECTIONS

American society values protecting privacy through control over personal information and, specifically, control over PHI.[128] However, this value is being challenged by the swift evolution of social networking. This area raises challenges in new and unfamiliar ways. Preservation of this value will require significant attention to this rapid evolution, and protection should be extended to PHI on social networking sites for two reasons. First, extending protections to PHI shared in social networking would respect realities ignored by current law. Second, without protections, the disconnect between expected and actual privacy will harm users through unanticipated PHI disclosures.

123. For examples of case law on point, *see, e.g.*,Cohen v. Facebook, Inc., No. C 10-5282 RS, 2011 WL 5117164 (N.D. Cal. Oct. 27, 2011); Fraley v. Facebook, Inc., 830 F.Supp.2d 785 (N.D. Cal. 2011).

124. *See supra* note 5.

125. 2000 Privacy Standards, *supra* note 11, at 82,464 ("Among different sorts of personal information, health information is among the most sensitive.").

126. *See id.*at 82,465 ("[M]alicious or inquisitive persons may download medical records for purposes ranging from identity theft to embarrassment to prurient interest in the life of a celebrity or neighbor.").

127. *See supra* note 5; *and* Prodhan, *supra* note 122.

128. *See supra* Part I.

A. Social Networking Realities

The swift evolution of social networking has produced four realities. First, social networking is on the rise.[129] Second, social networking is valuable.[130] Third, users expect that they have control over the information they share.[131] Fourth, this expectation of privacy is undermined by the sites' conflicting privacy representations.[132]

Social networking is on the rise.[133] Sites like Facebook,[134] Twitter,[135] and Google,[136] which have become ubiquitous, boast membership in the hundreds of millions.[137] Social networking has become a common method of interaction and shows no signs of abating.[138] One possible way to address harms incurred by sharing information online is to warn a user against posting anything that user would not want shared with the world, a "just don't post it" philosophy. However, while controlling personal information by not posting might be one way to fit into the current law, this is unrealistic and ignores social networking's pervasiveness.

---

129. *See, e.g.*, @Twitter, *supra* note 4 (detailing increases in Twitter users and accounts).

130. *See infra* notes 172-73 and accompanying text.

131. *See infra* notes 174-83 and accompanying text.

132. *See infra* notes 184-94 and accompanying text.

133. *See* @Twitter, *supra* note 4 (detailing increases in Twitter users and accounts).

134. *See* Monica Hesse, *Status Symbol: Facebook Is Ubiquitous, But Is It Really an Antisocial Network?*, WASH. POST. (July 23, 2010), http://www.washingtonpost.com/wp-dyn/content/article/2010/07/22/AR20100072206154.html (describing Facebook's massive popularity and prevalence in modern society).

135. *TWITTER: The Fastest Growing Social Platform*, GLOBAL WEBINDEX, http://globalwebindex.net/wp-content/uploads/downloads/2013/02/Twitter_GWI_2013.pdf (last visited Mar. 2, 2013) ("Twitter is now the fastest growing social platform increasing 40% between Q[uarter] 2 and Q[uarter] 4[,] 2012. This means there are now 485m[illion] account holders and 288 m[illion] active users.").

136. Richard Siklos, *Ubiquitious? Omniscient? It Must Be Google*, TELEGRAPH (Nov. 2, 2003 12:01 A), http://www.telegraph.co.uk/finance/2867734/Ubiquitous-Omniscient-It-must-be-Google.html (discussing Google and its history of privacy practices).

137. *See Key Facts*, *supra* note 3; *and* @Twitter, *supra* note 4.

138. *See* @Twitter, *supra* note 4 (showing the number of Twitter users growing each year).

Second, social networking is valuable. In today's internet-based society, social networking sites serve important roles—creating opportunities for building identity, dignity, and intimacy.[139] Social networking has also expanded beyond the social capacity, becoming a tool for business, marketing, news, and politics.[140] This trend continues to escalate, and accordingly, social media will likely continue to permeate interpersonal interactions.

Third, users expect that they have control over the information they share.[141] While there are disagreements over whether privacy can actually exist in the context of social networking interactions,[142] those who participate in social networks experience real feelings of protectiveness of their online "space" and the information they share in that space.[143] These feelings are supported by the sites' reassuring privacy jargon.[144] Sites market themselves as providing an opportunity to share personal information and develop personal relationships in a "trusted environment."[145] For example, Google recently launched a promotion for its Google+ platform, which includes "Circles."[146] Google promoted this feature as "sharing but like

139. Abril, *supra* note 19, at 83-87 (detailing four primary reasons for increasing online privacy protection: the promotion of identity; dignity; intimacy and socialization; and discourse).

140. Facebook Public Policy Europe, *Measuring Facebook's Economic Impact in Europe*, FACEBOOK NEWSROOM (Jan. 24, 2012), http://newsroom.fb.com/Whats-New-Home-Page/Measuring-Facebook-s-economic-impact-in-Europe-ae.aspx ("Citizens can now speak directly to their leaders, new political movements are born online, and a single voice can reach an audience of millions."). *See also*, @Twitter, *supra* note 4; *Tweet, tweet! Using Twitter to Build Career Connections Now*, *supra* note 6, at 8; Dysart, *supra* note 6, at 32.

141. *See, e.g.*, Levin & Abril, *supra* note 30 (demonstrating findings of an empirical study showing that users have expectations of privacy over what they share via social media).

142. Abril, *supra* note 19, at 73 ("[S]ome subscribe to the notion that online privacy is non-existent and its protection, whether legal or practical, is therefore futile.").

143. *Id.* (citing users' "feeling[s] of intrusion when their online personae are discovered by . . . unintended audiences").

144. *See, e.g.*, *Facebook Reveals 'Simplified' Privacy Changes*, *supra* note 3 (praising increased privacy settings options but criticizing overlooking sale of personal data to advertisers); *and* Bankston, *supra* note 3 (criticizing new Facebook privacy changes as "clearly intended to push Facebook users to publicly share *even more* information than before" and reducing user control over "personal data") (emphasis in original).

145. *See Fact Sheet*, *supra* note 112 (discussing how Facebook advertises its service as being able to interact with friends in a trusted environment).

146. *See Google*, *supra* note 8.

real life,"[147] purporting to allow users to selectively share information with only certain contacts, just as they would divide their social groups offline.[148] This approach equates cyberspace to real space, creating a feeling of security akin to sitting in a virtual living room talking to a set group of friends.[149] This sense of security in online sharing renders users vulnerable to unintended disclosures of information, especially when these very public advertisements are only part of the reality.[150]

Fourth, despite this emphasis on control and privacy, the reality is that much privacy control is subject to the sites' discretion.[151] For example, in addition to its "Circles" promotions,[152] Google has recently begun to alert users to impending changes in its privacy policy.[153] These changes include an increase in the information that is connected across various platforms[154]—without users' consent[155] or

147. *Id.* ("Sharing but like real life." quote appears at time code 1:21).

148. *Id.*

149. *See* Harvest Zhang, *Google+ and Circles: Why Keeping Social Groups Separate Is Highly Necessary and Why Facebook's Retaliatory "Friends Lists" Fail*, NETWORK20Q ELE 281 CLASS BLOG (Sept. 20, 2011, 3:16 PM), http://scenic.princeton.edu/network20q/blog/?p=61 (for an example of this perception).

150. *See, e.g.*, Miguel Helft, *Facebook Acknowledges Privacy Issue with Applications,* N.Y. TIMES (Oct. 18, 2010 11:58 AM), http://bits.blogs.nytimes.com/2010/10/18/facebook-admits-to-privacy-issue-and-makes-fixes/ (describing public response to Facebook giving users' personal information to advertisers and other third parties).

151. *See supra* note 5. *See also One Policy, One Google Experience*, GOOGLE POLICIES & PRINCIPLES, http://www.google.com/intl/en/policies/ (last visited Feb. 19, 2012) (explaining the upcoming compulsory change to privacy policy and terms of use).

152. *See Helft, supra* note 150.

153. Tim Carmody, *Google Streamlines Privacy Policy to Integrate Its Products*, WIRED (Jan. 24, 2012, 6:16 PM), http://www.wired.com/business/2012/01/google-streamlines-privacy/ (discussing Google's new integrated privacy policy and corresponding privacy alert system).

154. Tom McCarthy, *Google's New 'Tailored' Privacy Policy: How to Circumvent the Rules*, GUARDIAN, (Feb. 29, 2012, 3:18 PM EST), http://www.guardian.co.uk/technology/us-news-blog/2012/feb/29/google-privacy-policy-tips-and-tricks (When users are signed in to Google, the new policy will permit Google to "do things like suggest search queries – or tailor your search results – based on the interests you've expressed [in Google+, Gmail, and YouTube.]").

155. Mat Honan, *Google's Broken Promise: The End of "Don't Be Evil"*, GIZMODO (Jan. 24, 2012, 5:41 PM), http://gizmodo.com/5878987/its-

ability to opt-out.[156] Obtuse and convoluted policies make it more difficult to determine the level of control individuals retain over privacy settings and other users' access to their information. Not only are these policies dominated by legal terminology and difficult to understand, but scholars have also suggested that most users do not read them,[157] and, if they did, the opportunities cost for reading these policies would approximate $780 billion annually for American users alone.[158]

B. The Privacy Disconnect and Resulting Harms to Users

The disconnect between users' expectations of control of information in social networking settings and the reality of its limits are likely to result in a myriad of harms to users. Three examples provide a sampling of these potential harms.

First, consider the storage of information on social networking sites. Urban legend—backed by truth—tells that nothing can ever truly be deleted from users' online personas.[159] Facebook itself cautions users of this fact, noting, "Even after you remove information from your profile or delete your account, copies of that information may remain viewable elsewhere."[160] An individual could attempt to take control of his information by removing it from a social networking site, only to be frustrated by a programmed inability to achieve that goal.

---

official-google-is-evil-nowId. ("If you use Google's services, you have to agree to this new privacy policy.").

156. For the purposes of this note, "opt out" means zero-participation in or consent to the Google privacy policy. Google does assert that there are methods to "opt out" for certain mobile devices. *See Anonymous Identifiers on Mobile Devices*, GOOGLE, http://www.google.com/policies/technologies/ads/ (last visited. Mar. 3, 2013).

157. Aleecia M. McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, 4 I/S: J.L. & Pol'y for Info. Soc'y 543, 564-67 (2008–09) (discussing the costs associated with taking the time to read privacy policies).

158. *Id.* (advocating that an online privacy system requiring users to read lengthy and complex privacy policies to preserve their rights is too costly, and that companies should find ways to convey privacy practices "in useable ways, which includes reducing the time it takes to read policies").

159. For an illustrative example, *see* Internet Archive, *The Wayback Machine*, ARCHIVE.ORG, http://archive.org/web/web.php (last visited Mar. 3, 2013) (the "Wayback Machine" is an internet archive cataloging over 2 billion webpages).

160. McMillen v. Hummingbird Speedway, Inc., 2010 Pa. Dist. & Cnty. Dec. LEXIS 270, 6-7 (Pa. Cnty. Ct. 2010) (citing Facebook, http://www.facebook.com/policy.php (revised April 22, 2010)).

Next, consider changing privacy policies that result in disclosure beyond what the individual intended. Social networking sites' well-documented and contentious practice of changing their privacy settings seemingly overnight is just another of the potential snares for social networking users.[161] These changes are often implemented without significant warning or user input, and often go into effect before users are aware of them.[162] Google's recent privacy changes provide an example.[163] Users have the benefit of advanced notice in this instance, but lack the ability to opt-out of the increased cross-platform sharing of information.[164] Many sites have not afforded users the same level of alerts before a change in policies.[165] For example, Facebook has a history of changing privacy settings in such a way as to render privately held information public.[166]

Privacy setting changes of this nature can mean that an individual user may have taken all the available protective steps, but still have their personal information disclosed beyond their intended audience. While the recent Federal Trade Commission (FTC) settlements address these issues retrospectively,[167] the threat of future disclosures from social networking sites remains. Although the settlement agreements place stringent privacy requirements on Facebook and Google for the next twenty years, these requirements

161. Discontent with such practices has seen discussion for several years. *See supra* note 149 Meanwhile, there has been no resolution until the recent settlement agreement with the F.T.C. *See* Protalinski, *supra* note 3 (discussion the settlement).

162. *See, e.g.*, Low v. LinkedIn Corp., 11-CV-01468-LHK, 2012 WL 2873847 (N.D. Cal. 2012) ("As noted by Defendant, although the Amended Complaint describes the terms of Defendant's privacy policy in detail, Plaintiffs never allege that they were aware of the privacy policy, let alone saw or read it.").

163. *Privacy Policy*, GOOGLE (July 27, 2012), http://www.google.com/policies/privacy/.

164. *Id.* (noting failure to provide a means for opting-out of information sharing).

165. *See, e.g.*, McVicker v. King, 266 F.R.D. 92, 96 (W.D.Pa. 2010) (discussing implications of website privacy policy); *see also FTC Gives Final Approval to Settlement with Google over Buzz Rollout*, FEDERAL TRADE COMM'N (Oct. 24, 2011), http://www.ftc.gov/opa/2011/10/buzz.shtm (noting that even Google did not provide such alerts to its users before rolling out its social networking feature, Buzz, in 2010, providing the impetus for the charges and recent settlement with the F.T.C).

166. *Cf.* Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965, 991 (C.D. Cal. 2010) (determining whether [plaintiff's] privacy settings rendered [his] wall postings and comments public).

167. *See* Protalinski, *supra* note 3 (discussing the settlement).

are based on harms from site components that are, in several instances, already obsolete.[168] This rapid change further illustrates the need for protections based on categories of information and not on specific technological practices.

Fourth, consider the sale of information to third party sites, a practice that has been going on behind the scenes for years.[169] Sites have advertised privacy controls to users while selling or otherwise distributing information outside the realm of the social networking site.[170] This practice results in personal information being spread far beyond users' expectations or awareness.

From the control-as-privacy perspective, the storage, compromise, and sale of information in social networking give cause for concern. In the future, what will social networking sites do with stored information? What if the site is compromised or sold? What if a user takes all available precautions, or sends information in a private message, and the information is still compromised?

Current law does not provide a satisfactory answer to these potential problems. The fact remains that information spread through online social networking can reach beyond the intended audience.[171] Ignoring the hazards the online world poses will not protect individuals, their privacy, or their PHI; these threats must be confronted. The recent FTC settlements with Facebook and Google validate both the reality of these harms and the legitimacy of the users' interests.[172] Courts and legislatures, however, have not kept pace with these expectations,[173] and retrospective solutions such as the FTC settlements offer insufficient protection.[174] Bridging this gap will

168. *Id.*

169. *See supra* note 149.

170. *See supra* note 149.

171. For example, the capacity to "retweet" information can send a post viral. *See* Dan Zarrella, *The Science of ReTweets*, MASHABLE (Feb. 17, 2009), http://mashable.com/2009/02/17/twitter-retweets/ (analyzing how Twitter posts go viral).

172. *See* Protalinski, *supra* note 3 (discussing the settlement). *See also In the Matter of Google, Inc.,* Federal Trade Comm'n, File No. 102 3136, *available at* http://www.ftc.gov/os/caselist/1023136/110330googlebuzzagreeorder.pdf.

173. *See, e.g.*, McMillen v. Hummingbird Speedway, Inc., 2010 Pa. Dist. & Cnty. Dec. LEXIS 270 (Pa. Cnty. Ct. 2010) ("The relationships to be fostered through those media are basic friendships, not attorney-client, physician-patient, or psychologist-patient types of relationships, and while one may expect that his friend will hold certain information in confidence, the maintenance of one's friendships typically does not depend on confidentiality.").

174. *See* Protalinski, *supra* note 3 (discussing the settlement).

require more than retrospective causes of action based on the antiquated constraints of physical space and applied to artificial boundaries—it will require a national solution in the form of preventative federal regulations that can adapt to the current and developing problems of protecting PHI in social networking.

IV. PROPOSED SOLUTION: FEDERAL REGULATIONS

Americans value protection of privacy.[175] Americans also value preserving individual control over PHI.[176] Social networking is ubiquitous and is here to stay.[177] This three-way confluence of privacy values, PHI protection, and expansion of social networking is an intersection in which problems will develop if not given proper attention.[178] While online social networking has positive aspects,[179] its potential dangers should be addressed preemptively. With the lack of meaningful protections from current federal regulations and state laws,[180] there is a strong need for forward-thinking, preventative measures to protect this highly valued, vulnerable category of information. This Part first discusses how a comprehensive set of federal regulations could fill this need. Next, it outlines the advantages of this regulatory solution.

A. Proposed Regulations

To more effectively protect personal health information shared in online social networking settings, HHS should build on the "floor" described in the HIPAA Privacy Rule and promulgate additional federal regulations.[181] In designing these regulations, HHS should allow individuals to retain a right of control over their personal health information by virtue of the character of the information itself.

One of the arguments against federal regulations for privacy protection of information shared in social networking is that this industry's vast scope would make the regulations impossible to enforce and therefore render them powerless.[182] A similar criticism

175. *See supra* Part I.

176. *See supra* Part I.

177. *See supra* Part III.A.

178. *See supra* Part III.

179. *See supra* Part III.A.

180. *See supra* Part II.

181. Privacy Standards Modifications, *supra* note 40, at 53,182 ("[T]he Privacy Rule creates, for the first time, a floor of national protections for the privacy of [consumers'] most sensitive information—health information.").

182. *See, e.g.*, Terry, *supra* note 76. *See also* Gilman & Cooper, *supra* note 24.

was advanced against the recently proposed data laws in the European Union, arguing the standards imposed would prove too difficult for compliance.[183] Accepting the premise that "it would be nearly impossible to trace all the places information may have spread after disclosure"[184] underscores the need for preventative components to the proposed regulations. However, if the regulations were modeled on the value of protecting PHI based on its inherent characteristics, they would be able to regulate use of the information for broad categories of actors by providing guidance before inappropriate disclosure occurs.

Because the regulations would address uses pertaining to PHI, HSS should bear the responsibility of drafting and promulgating the regulations. As the agency with the most experience handling issues related to PHI,[185] HHS is best equipped to draft informed, meaningful regulations in this area. The definition of PHI should be similar to that articulated under HIPAA.[186] PHI should be defined as any information that relates to the past, present, or future physical or mental health or condition of an individual.[187] This includes a wide range of information that could be identified through filters and screening processes by the sites. Examples include, but are not limited to, an individual posting about a physician appointment, the cold they had last week, a friend's surgery, or other health-related postings. As part of the regulations, HHS should establish administrative tribunals responsible for hearing complaints under these regulations.

These regulations should employ a three-pronged approach. First, the regulations should require meaningful privacy disclosures and truthful advertising from social networking sites. Second, the regulations should provide guidelines for the use of any PHI shared and collected on social networking sites. Third, the regulations should establish several courses of action and meaningful remedies for

183. *See* Prodhan, *supra* note 122 (discussing the likelihood that enforcing new E.U. data-protection proposals will be difficult, due in part to inability to trace and totally remove contested information).

184. *Id.*

185. HHS promulgated both the HIPAA Privacy Rule and the HITECH Act, both dealing with PHI. *See* 2000 Privacy Standards, *supra* note 11, at 82,462. *See also* HITECH, *supra* note 25.

186. HIPAA Privacy Rule, *supra* note 25, at § 160.103.("Health information means any information, whether oral or recorded in any form or medium, that . . . [r]elates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual.").

187. *See id.*

both individual social networking users and for social networking sites.

1. *Meaningful Privacy Disclosures and Truthful Advertising*

The first prong of the regulations should require social networking sites to make meaningful, plain language privacy disclosures and to be truthful in how they advertise users' control over privacy and use of information. While there are many different ways this could be accomplished, this Note proposes four "first steps" toward achieving this goal.

First, sites should be required to make their privacy policies more accessible to users. This could be accomplished by making the privacy policies easier to find and understand. The sites should be required to make the link to their privacy policies more prominent on the site. Users should not have to painstakingly search for the website privacy policy to find it. The policies should also be accessible in a meaningful, plain language way. While the importance of legal terminology in these policies cannot be overlooked, the privacy policy should be supplemented by a version that a layperson could easily read and understand. Access to the policies in plain language is necessary for users to make meaningful decisions regarding the protection of their PHI. This access should include notification—also in plain language—that alerts users to any pending changes in the privacy policy.

Second, users should be required to complete a series of uncomplicated procedures before creating a profile. Initially, the user should have to undertake a comprehensive review of the privacy policy, rather than simply selecting a check box and clicking "I Accept." This could be accomplished in the form of a short plain-language document that pops up, highlights, and then explains the site's privacy policy and terms of use. Following review of this document, users would be required to complete a short quiz; passing the quiz would demonstrate an adequate understanding of the ways the users' personal information will be used. Such a review and quiz process could also be required for each user on a regular basis, or each time the site changes its privacy policy or terms of use. A notice that policies are changing is of little utility if users do not read or fail to understand the policies. This tutorial should also be available to the users any time they desire a refresher on how the site is permitted to handle their information.

Third, the sites should be required to undertake a similar process explaining and highlighting the user-controlled privacy settings of the site. Four requirements would help achieve this goal. First, sites should be required to make these explanations and settings transparent, meaningful, and user friendly. Second, sites should be required to make profiles' default setting private, not public. Third, the sites should not be permitted to change a user's privacy settings

without the user's affirmative authorization. In addition to the pop-up privacy policy review, any change in user-controlled privacy settings should be subject to a similar walkthrough and would be at the user's discretion to accept or reject. Finally, sites should be required to give users the ability to flag or mark information as sensitive PHI that they do not want to be distributed, and the site should be required to review that information before proceeding with its use or distribution.

The fourth initial step would require social networking sites to be truthful in their advertising.[188] Sites should have to issue a disclaimer that users should review the sites' privacy policies before posting information. Sites should also be prohibited from advertising misleading levels of control over privacy and information. Depending upon the advertisement medium, any advertisement should have to be accompanied by a plain-language notice that is either visible or audible and in the same language as the predominance of the advertisement. A site's advertisement should not leave a user with an inaccurate understanding of the privacy or control their posts are afforded.

2. *Guidelines for Use of Personal Health Information*

The second prong of the regulations would establish guidelines for the use of any PHI shared and collected on social networking sites. Attaching protection to the information itself would be more meaningful and long lasting than trying to regulate the fast-paced evolution of the technology, while also respecting the intrinsic value and basic premise of social networking.[189] Current federal protections already take the approach that the PHI itself deserves protection[190] and apply regulations to broad categories of health care industry actors.[191] Regulating social networking sites' use of PHI could follow HIPAA's approach to regulating "covered entities."[192] By the same approach, regulating the vast network of other firms, advertisers, data

188. This portion of the regulations should be developed by HHS in conjunction with the FTC. so that the expertise of both agencies could be incorporated into this pivotal provision. For a summary of each agency's areas of expertise, *see About the Federal Trade Commission*, Fed. Trade Comm'n, http://www.ftc.gov/ftc/about.shtm (last visited Mar. 14, 2013); *What We Do*, U.S. DEP'T OF HEALTH AND HUMAN SERV., http://www.hhs.gov/about/whatwedo.html/ (last visited Mar. 14, 2013).

189. *See supra* Part III.A.

190. *See supra* Part I.

191. *See supra* Part II.A.

192. *See supra* Parts I, II.A.

storage companies, and so forth, is akin to regulating "business associates."[193]

The regulations would provide guidelines to social networking sites on what is permissible use of PHI. Social networking sites should not be allowed to collect or distribute this PHI from user's profiles and interactions. The only exception to this would be if the sites de-identified the information and no longer linked it to the individual or his online profile or persona. The de-identified information could be collected and used for research purposes, but directed advertisements should not be allowed unless requested by the user.

The regulations should also provide guidelines to third party companies that gather or receive information from social networking sites. PHI should be a protected category of information that cannot be used for marketing, advertising, or further distribution, unless the user grants specific, informed consent. Just as the HITECH Act gives individuals the right to know who has accessed their PHI,[194] the proposed regulations would confer a similar right. Once PHI is collected and distributed outside the realm of the social networking sites themselves, users would have a right to know who else has accessed that information. Third party companies—the "business associates" of social networking sites—would still be responsible to the users based on the nature of the PHI.

3. *Available Actions and Remedies*

Implementing the above-mentioned privacy disclosures and regulations would establish a framework that would decrease the incidence of harm to users from PHI disclosures. It would establish much of the needed preventative protection and decrease reliance on less effective retrospective remedies. However, in recognizing that not all harms can be prevented, the third prong of the regulations should establish several courses of action and meaningful remedies for both individual social networking users and social networking websites.

The regulations should also create a cause of action for individuals whose PHI has been inappropriately disclosed by social networking sites or their third party affiliates: "wrongful distribution of PHI." Such a cause of action would abandon the constraints of traditional causes of action and their focus on physical space.

The initial step in pursuing this cause of action should be for the user to request an administrative preliminary injunction. A social networking user who suspects his PHI has been compromised would

193. *See supra* Parts I, II.A.

194. HITECH Act,, 123 Stat. 230, P.L. 115-5, §13405(c)(1)(B) (codified as amended 42 U.S.C. 17935) ("an individual shall have a right to receive an accounting of disclosures. . .").

file a complaint with the administrative tribunal in his jurisdiction designated to hear these complaints. This tribunal should evaluate the claim in the light most favorable to the individual and could then issue a preliminary injunction, requiring the accused site or affiliate to remove or cease use of the contested information. The administrative tribunal should then issue an opinion on whether the information qualifies as PHI and, if so, whether it has been inappropriately used or disclosed. These opinions should be published for precedential value on which users, social networking sites, and decision-makers in the other tribunals could rely.

Both parties would be entitled to appeal through a separate agency arbitration process. The decisions of these arbitrations should be reasoned awards, explaining the facts and reasons for the decision and should be available as precedent to the tribunals. If the individual prevailed, he should be entitled to damages as calculated for pain and suffering and/or damage to reputation.[195] The social networking site or third party affiliate should be required to stop using the contested information. Further, the site should be required to contact any other sites to which they distributed the information to alert them to stop using the information. It should remain up to the individual's discretion whether to keep the information posted on his social networking page, but the site should not be allowed to use that information. If the social networking site prevailed, however, it would be entitled to use the information. Finally, appeal to the courts would be available to the individuals and social networking sites.

In addition to the cause of action established primarily for the benefit of individuals, there should also be a course of action available to the social networking sites themselves that would aid in understanding the limits imposed by the regulations. Sites should be permitted to request a "ruling letter" from HHS to evaluate proposed uses and disclosures of information. These ruling letters should serve as advisory opinions, and could provide another preventative avenue for decreasing harms to users. Such preventative measures would further decrease the need for retrospective actions.

B. Advantages of the Proposed Regulations

These proposed regulations provide three primary benefits. First, the regulations would fill the current gap in the law between the realities of social networking and protections for PHI. Second, they would provide a meaningful process to resolve disputes and obtain remedies. Third, and most importantly, they would set out clear expectations for all parties involved in social networking and help

195. This is similar to the damages available for the tort of defamation. *See* RESTATEMENT (SECOND) OF TORTS § 621 (1977).

preempt disputes. Together, these benefits would result in an online environment that aligns with users' current expectations, meaningfully guides businesses and courts, and sets precedent to inform future discussions as other similar issues arise.

1. *Fill the Current Gap in the Law Between the Realities of Social Networking and Protections for PHI*

The proposed regulations would bring protection for PHI shared in social networking forward from where HIPAA and HITECH stopped short. They would also eliminate the need for the fragmented and outdated state protection. The proposed regulations would fill the gap that has resulted from the convergence of privacy values, the value placed on PHI, and the rapidly evolving area of social networking.

PHI shared in social networking interactions is currently unprotected and therefore vulnerable, especially through third-party use. If an individual divulges PHI, even if in a forum that is not as "traditionally" private as others are, the information still retains the inherent character that American society feels strongly should be protected. The proposed regulations would update the law to effectuate this value.

2. *Afford Meaningful Dispute Resolution Options and Remedies*

Meaningful remedies do not just mean satisfaction to an injured plaintiff; they also entail remedies that reflect the context in which the wrong was committed.[196] The proposed regulations outline an efficient process for dispute resolution that recognizes the unique character of wrongs in a social networking context. This approach results in simplicity, uniformity, and consistency of remedies to the advantage of all parties involved.

The proposed regulations ensure that decision-makers—the administrative tribunals, arbitrators, and courts—would have precedent on which to base their decisions. Complicating the current ability to shape meaningful remedies is the phenomenon of the "vanishing trial."[197] With more and more disputes resolved through private methods of alternative dispute resolution, the number of precedential decisions from the courts has diminished, especially in the social networking context; this, in turn, has diminished the

196. See Tracy A. Thomas, *Ubi Jus, Ibi Remedium: The Fundamental Right to A Remedy Under Due Process*, 41 SAN DIEGO L. REV. 1633, 1642 (2004) (discussing what makes a meaningful remedy).

197. Thomas J. Stipanowich, *ADR and the 'Vanishing Trial': What We Know—And What We Don't*, 10 DISP. RESOL. MAG. 7 (Summer 2004) (explaining why alternative dispute resolution methods are decreasing the frequency of trials).

influence jurisprudence has on shaping social norms involving PHI.[198] The proposed regulations would provide decision-makers with a foundation based in the reality of online social networking and not in antiquated understandings of privacy based on physical space. Requiring published, reasoned awards would provide structure and bridge the gap left by diminishing precedential opinions.

3. *Preempt Disputes Through Clear Expectations for All Parties Involved*

Perhaps the most meaningful impact stemming from these proposed regulations is that they would convey clear expectations for the use of PHI disclosed in social networking. Understanding what is expected regarding PHI would inform and guide the conduct of users, the social networking sites and third-party affiliates, and would help to preempt disputes.

The proposed regulations would comport with many of the expectations already held by online social networking users.[199] In addition to meeting current expectations of privacy, meaningful privacy disclosures would set realistic expectations for social networking users of what is and is not protected in their online interactions. The combination of knowledge and proposed regulatory protections would provide for more control over that information. This paradigm would give users confidence in knowing both the boundaries of protection and the limits on how their PHI can be used, as well as comfort in knowing there are penalties for inappropriate use and disclosure. It would also place a burden of responsibility on users; as they are more informed, they will be expected to participate in the responsible management of their PHI. The proposed regulations would set clear expectations for users and encourage informed participation in protection of PHI.

Social networking sites and their third-party affiliates would also benefit from the clear expectations set out in the proposed regulations. Understanding what is permissible regarding PHI would decrease the amount of confusion and litigation. Sites would be better able to protect against liability by complying with the regulations. As a result, they would be spared the costs—of money, time, and reputation—of litigation arising from a lack of legal guidelines.[200]

198. *Id.*

199. *See supra* Part III.A.

200. Preemption of disputes and the proposed resolution process would save judicial resources as well.

V. FURTHER IMPLICATIONS

Addressing the emerging issue of privacy for PHI in online social networking will not only align with users' current privacy expectations and quell worries about inappropriate disclosure, but also assist in resolving similar problems in the future. This Note has focused on PHI specifically, but the proposed regulations could also serve as a framework for other categories of information deemed worthy of protection. Similarly, this focus can be expanded beyond social networking to address concerns about the practices of data mining and usage generally.[201]

CONCLUSION

Social networking challenges the value American society places on PHI protection as a highly vulnerable category of information. With HIPAA, the HITECH Act, and their attendant regulations confirming this value,[202] the need for protections in social networking cannot be overlooked. The reality of social networking's ubiquity, popularity, and rapid evolution renders arguments such as "just don't post it" moot.[203] PHI disclosure has a unique potential for negative consequences; embarrassment, discrimination, and damage to relationships are but a few of the potential harms.[204] Forward-looking, preventative federal regulations will provide the most protection for PHI shared in a social networking context.

Current regulations do not extend into this area.[205] Additionally, the law varies state to state, ignoring the reality that social networking is unrestricted by geographic borders.[206] Similarly, frameworks rooted in a concept of physical space are a poor fit for wrongs in the online world.[207] Finally, retrospective rather than proactive schemes are insufficient to address the potential damage through inappropriate disclosure of PHI online.[208] Waiting to address

201. Another area where these regulations could have a positive impact would be in patient-managed electronic medical records. As patients increasingly begin to manage their own patient records electronically, significant access and disclosure issues will arise. *See* Terry, *supra* note 76 (outlining a framework to address issues between doctors and patients regarding electronic medical records).

202. *See supra* Part I.

203. *See supra* Part III.A.

204. *See supra* part I.

205. *See supra* part II.A.

206. *See supra* Part II.B.1.

207. *See supra* Part II.B.2.

208. *See supra* Part II.B.2.

the problem until information is inappropriately disclosed results in little opportunity for a meaningful remedy.

Federal regulations would protect the value placed on control of PHI by attaching protection to the information itself. It is more realistic to place restrictions on what can be done with acquired information than to attempt detailed regulation of this rapidly evolving industry.[209] While users should also participate in the protection of their personal information through use of the privacy settings afforded, deceptive privacy advertisement and obtuse privacy policies should not render this participation meaningless. Preemptively establishing a set of federal regulations as a benchmark for addressing these kinds of issues before they arise will help mitigate the harms that are otherwise sure to follow. Federal regulations requiring meaningful privacy disclosures and truthful advertising, establishing guidelines for use of PHI, and providing causes of action with precedential value would keep pace with reality of the evolution of online social networking.

Federal regulations protecting PHI would fill the gap in the current law, provide meaningful dispute resolution options and remedies, and delineate concrete expectations for all participants. The permanence of information posted online heightens the need for this sort of protection.[210] It is all too likely that information posted will become a permanent part of an individual's "digital" persona without the mercy of short human memory.[211] Such a framework will have broad applicability as more and more interactions move toward online exchanges.

209. *See supra* Part IV.A.

210. *See supra* Part III.B.

211. Abril, *supra* note 19, at 75 (discussing how "the digital record has increased the stakes of privacy today. . .").