August 13, 2009

Physicians And Patients Who “Friend” Or “Tweet”: Constructing A Legal Framework For Social Networking In A Highly Regulated Domain

Nicolas P Terry

Available at: https://works.bepress.com/nicolas_terry/1/
Abstract: Social networks connect intimates, friends, and acquaintances that share history, strangers who share interests, or businesses and the customers they serve. This article explores how participation in online social networks blurs the boundaries between personal and professional relationships or commentary, while making available “private” information in what only appears to be a secluded area. These issues are explored within the framework of the highly regulated health domain, casting doubts on the appropriateness of some professional activities and identifying considerable risks for patients and their health-related information.

I. Introduction ................................................................. 2

II. Social Networks ............................................................ 4
    A. Properties of Social Networks ......................................... 5
    B. Use, Perceptions, and Expectations .................................. 7
    C. Social Network Privacy and Security Settings ...................... 9

III. The Legal (and not so Legal) Framework .......................... 12
    A. Options; Property, Liability, Inalienability, and Soft Law ........ 14
    B. The Law of Boundaries; Privacy Torts and Breach of Confidence ...... 16
    C. Privacy Expectations & Social Networks .......................... 20
    D. Privacy and Confidentiality in Healthcare ............................ 22
    E. Ethical Restraints ................................................... 28
    F. HIPAA and Related Regulatory Models ............................... 30

IV. Setting Boundaries for Physicians and Patients .................. 32
    A. Physicians’ Social Information Online ............................... 33
    B. Patients’ Health-Related Information Online ....................... 35
    C. Physicians and Patients as “Friends” ............................... 42

* Copyright © 2009, Nicolas P. Terry. All Rights Reserved.
** Chester A. Myers Professor of Law, Senior Associate Dean, Professor of Health Management & Policy, Saint Louis University. Email: terry@slu.edu. I thank Leslie Francis for her helpful suggestions on an earlier draft and Michael Kella, SLU J.D. candidate 2011, for his research assistance.
INTRODUCTION

Computer-mediated social network sites are omnipresent and among the most popular of all web destinations. There seem to be few limits on who is posting or the subject matter of posts, and there is scant guidance on the appropriate limits for online social interactions. Originally, such sites were the exclusive playground of teenagers and college students (who continue to be the majority of users). Not surprisingly given this original demographic, media and legal scrutiny has tended to concentrate on the potential of such sites to enable child predators, facilitate other abuses of children and young adults such as bullying, and encourage “graffiti” behavior in adolescent users.

Although teenagers and young adults remain the dominant groups using social network sites, adult usage quadrupled between 2005 and 2008 as adults migrated to Facebook and MySpace initially, perhaps, to connect with their children and grandchildren. By December 2008 35% of online adults had used a social network site. Of course, all users do not equally enjoy all social network activities. For example, updating one’s personal status using Twitter or, say, Facebook’s “What’s on your mind?” feature...
continues to be an activity dominated by young adults.\(^9\)

Online social networks are increasingly attracting the attention of large and small businesses and professionals as vehicles for advertising, marketing, and providing customer support.\(^10\) For example, 54 percent of attorneys belong to an online social network,\(^11\) although membership remains skewed towards younger professional users.\(^12\) As the demographics of and motivations behind participation in social networks evolve, so the foundational teenager vs. teenager relationships and inevitable disputes will be replaced by more complex relationships and risks that are considerably more nuanced.

This article focuses on one highly complex relationship, that of physician and patient. That relationship, together with the related imperative of protecting patient information, constitutes a crucial component of the legal domain applicable to our most highly regulated industry. Recent inquiries into the trust and confidence properties of the physician-patient relationship and the protection of patient data have concentrated on the technical (diagnostic, pharmacy, etc.) data associated with the care relationship. Thus, questions have been asked about the adequacy of protection for networked or interoperable electronic records.\(^13\) Such inquiries have escalated as patients have been encouraged to leverage technology to store their own “personal” health records.\(^14\) This article is less interested in technical medical data and more with social data that implicates health and health-related decision-making. Here, the inquiry is how our legal, ethical and regulatory models will react as the social network phenomenon overlaps.

---


\(^12\) Id. Reporting membership of 25-35 (67%), 36-45 (49%), and 46-55+ year olds (36%).


with traditional healthcare relationships and businesses.

The analysis draws on the limited extant law dealing specifically with social network interactions and the law and ethics literature dealing with existing computer-mediated interactions between physicians and patients. The legal analysis principally is concerned with privacy and confidentiality constructs, described below as the “Law of Boundaries.” The article explores how participation in online social networks may blur boundaries between personal and professional relationships or commentary, while making available “private” information in what only appears to be a secluded area. The article also examines the potential for amelioration of risks with the currently under-utilized privacy and security settings provided by the online social networks.

The law of boundaries is applied to some specific scenarios where category breakdown may be detected: (1) physician social information online, (2) patient health-related information online, (3) physicians and patients as “friends,” and (4) physicians “tweeting” or posting about their work. These online scenarios challenge the perceptions, expectations, and sense of trust that are the properties of the offline physician-patient relationship. The application of legal, ethical, and regulatory models to these “worlds collide” phenomena casts doubts on the appropriateness of some professional activities and the online social activities of some physicians. Additionally, the article identifies considerable risks run by online patients who post about or otherwise signal their health status. Among several conclusions applicable to these social network scenarios it is suggested that the law of boundaries must evolve to protect non-public data or secluded areas established by users of social network sites.

II. Social Networks

The most popular social network sites include Facebook, MySpace, Twitter, and LinkedIn. Facebook has in excess of 150 million users and its subscribers spend more than 3 billion minutes per day on the web site. Of these services Twitter is currently showing the largest growth. Eleven percent of online American adults use Twitter or features on social network service sites to share information or read “updates” from others. The use of social network sites is now so pervasive that we may well be on our way to what Anita Allen has described as “the technological conceit of twenty-first century ‘lifelogging.’”

Our contemporary concept of social networking is a subset of computer-mediated (or computer network-mediated) communication. This latter, broader term includes

---

17 Id.
18 Pew, Twitter, Feb. 12, 2009 at 2.
email, blogs, web sites, and instant messaging. These extant models of computer network-mediated communication will inform the discussion that follows. However, they lack the distinctive features of social network services.

A. Properties of Social Networks

According to one court, “Online social networking is the practice of using a Web site or other interactive computer service to expand one’s business or social network.”

Boyd and Ellison provide a granular definition: “web-based services that allow individuals to (1) construct a public or semi-public profile within a bounded system, (2) articulate a list of other users with whom they share a connection, and (3) view and traverse their list of connections and those made by others within the system.”

There are two broad categories of computer-mediated social networks. First, there are those, like LinkedIn, that emphasize professional or business networking. Second, there are those, such as Bebo (a site popular in Europe), MySpace, and Facebook, which leverage the ‘social’ or friendship properties of pre-existing, predominately offline networks of intimates, friends, and acquaintances.

Boyd and Ellison explain this distinction between networking and networks as follows:

What makes social network sites unique is not that they allow individuals to meet strangers, but rather that they enable users to articulate and make visible their social networks. (P)articipants are not necessarily “networking” or looking to meet new people; instead, they are primarily communicat-

---

20. A more expansive list of social network services or sites could be drawn-up. For example, for some the fact that viewers rate content on YouTube, share opinions about products on Amazon.com, or rate each other on eBay.com might qualify these sites as social networks.


23. “LinkedIn is an interconnected network of experienced professionals from around the world, representing 170 industries and 200 countries. You can find, be introduced to, and collaborate with qualified professionals that you need to work with to accomplish your goals.” http://press.linkedin.com/about

24. Bebo is a popular social networking site which connects you to everyone and everything you care about. It is your life online - a social experience that helps you discover what’s going on with your world and helps the world discover what’s going on with you.” http://www.bebo.com/StaticPage.jsp?StaticPageId=2517103831


26. "MySpace is a place for friends... MySpace is Your Space... MySpace keeps you connected..." http://www.MySpace.com/index.cfm?fultsection=usrourhome

27. "Giving people the power to share and make the world more open and connected.” http://www.facebook.com/home.php?ref=login#/facebook?ref=pf
ing with people who are already a part of their extended social network.\(^2^8\)

Thus, a typical LinkedIn subscriber seeks to leverage the contacts of contacts to increase the range of their professional networking. However, a Facebook user primarily seeks to communicate with an existing network of “friends” and, only incidentally (or at least initially), leverage the virtual networks of his or her friends to identify (and then “friend”) participating friends from their existing real world network.\(^2^9\) Empirical data seems to bear out this distinction. Adults use professional sites sparingly (e.g., six percent of adults use LinkedIn), but they use them almost exclusively for professional purposes. Social network sites such as Facebook and MySpace see more mixed use, though adults tend to use them far more for social purposes.\(^3^0\)

The reason for drawing this admittedly imprecise distinction between the two types of service is that these uses or functions will tend to drive differential expectations of privacy, confidentiality, and appropriateness of communications. It is assumed, for example, that those who participate in true professional networking services will tend to be more guarded and finite in their engagements. In contrast, those who post or share “what’s on [their] mind” on Facebook generally do so with the expectation that they are communicating with a group of friends, an extant social group. Although “social networking” and “social network” services function quite similarly, this article concentrates on the latter group. As such, it ignores social network sites designed solely for healthcare professionals\(^3^1\) or those that cater to specific diseases or illnesses.\(^3^2\)

A user of a social network site registers with the service and then creates a profile. This profile functions as the link between the user’s real world and virtual world personas. This profile may include a variety of rich media including photographs, videos, and links. Typically, the service will have some kind of search engine (or an automated one keyed to email addresses) that will discover existing real world friends who have a virtual presence in the social network. Usually, a user can opt-out from being so discoverable. Once a user identifies someone with whom they wish to virtually network, they send (e.g., in Facebook) a “friend” request. The network loop is not established until the
A putative friend accepts that request.\footnote{See generally boyd & Ellison, supra note 22.}

Twitter\footnote{See generally boyd & Ellison, supra note 22.} is very similar to the character-limited news feed ("What's on your mind?") popularized by Facebook. However, it differs from other social networks because its users are less likely to restrict the viewing of their posts to a restricted group of existing contacts (although that is possible\footnote{Just as it is possible, but less likely, that a user will open his or her Facebook page to the public.}). Users of Twitter "tweet" in bites of up to 140 characters what they are doing or thinking at any particular time. Other Twitter subscribers may then "follow" these postings. Thus, those who are interesting because they are famous, or famous because they are interesting, have their posts "followed" by other subscribers, frequently in far larger numbers than, say, Facebook friends. Thus, Twitter shares characteristics with web (particularly blog) sites in that it tends to operate as a broadcast or one-to-many service. As predominantly used, Twitter lacks a key property of other popular social networks in that the publisher of a message typically will not control who can see that post (i.e., it is "one-directional" rather than "bi-directional"\footnote{boyd & Ellison, supra note 22.}); although it does resemble a service such as Facebook in that the consumer can choose whether or not to subscribe to posts from that other user.\footnote{The terrain is further complicated by interactions between these services. For example, Twitter users can link their "tweets" to Facebook so that they are displayed in Facebook as news feeds. See Facebook Tweeter, http://www.facebook.com/apps/application.php?id=16268963069, (last visited Jul. 10, 2009).}

B. Use, Perceptions, and Expectations

Basic Internet communication tools are either limited in their reach or obvious as to their broadcast nature. Notwithstanding the occasional breakdown when a user ill-advisedly clicks "reply to all" or "reply" on a listserv, email is and is perceived to be a one-to-one communication. In practice, email may be no more private than sending a postcard through the mail (potentially it could be read by many), but in practice few postcards are read by unintended recipients. At the other extreme, the publisher of content to a web page or a traditional blog should realize that this is a one-to-many broadcast.

cation, and networking tools allow those online to apply a virtual overlay to their offline lives. Thus, a user who enters an address into Google Maps creates a representation of that real place. When that user enables location services on a mobile device and allows the online service to share that data with others, the user’s real and virtual world locations are overlaid. Similarly, when a user converses on a social network service he or she is mapping her virtual conversation to his or her real network of friends and acquaintances. In Facebook-speak this is referred to as “the digital mapping of people’s real-world social connections.” However, the potential consequences of such virtual communication are of a different order.

Real world (or offline) communications are beset by inefficiencies and “noise” that have the effect of limiting the reach of the participants’ communications. The context of the listening group (for example, an audience of intimates or co-workers around the water-cooler) will (or should) modulate the content of the conversation. Social network services break this paradigm because they encourage and operationalize the posting of intimate or private moments or thoughts on the user’s news feed, “wall,” or in a “tweet.” Services such as Facebook confuse the communication model for the user and potentially lead to category breakdown because they offer the opportunity for apparently one-to-one conversations (e.g., a “wall” comment) that are nevertheless open to all in a group (a broadcast context).

This initial category breakdown (or state of pseudo-seclusion) is exacerbated in online social networks because the smaller (inefficient) and segregated social categories we tend to have in the real world (relatively distinct categories of intimates, co-employees, co-professionals, etc.) may become blurred when we create larger aggregated “friend” groups from several categories. For example, a Facebook user’s network of “friends” likely will start with a small number of intimates. However, as the social network service’s tools for “finding” “friends” are used (e.g., allowing Facebook to mine one’s Gmail address book, or “friending” mere acquaintances who are friends of friends) the properties of the “friended” group may have changed dramatically to include co-workers, employers, or customers.

It may be the case that users of social network sites are “quite oblivious, unconcerned, or just pragmatic about their personal privacy.” Equally, such users may be willing to knowingly trade their private information (usually only shared with intimates) in order to increase their number of “friends” and build new online or offline relation-

---

In their study of information sharing on Facebook, Gross and colleagues examined the tenuous application of social network theory to online networks. As they observed, although "offline" social networks may consist of extremely diverse relationships from intimates to acquaintances, online networks can "reduce these nuanced connections to simplistic binary relations: 'Friend or not.'" While the context changes as the user moves from offline to online discourse and data sharing, the user may not be fully aware of the category blurring and fail to appropriately modulate the content.

Social network services also impact how users interact with their posted data or content due to a shift from taxonomy (top-down indexing by experts or content owners) to folksonomy (bottom-up indexing or "social tagging" by users). Consider the participant in our water cooler conversation who shows a recently taken photograph to the other participants. Our participant likely will contextualize the image (e.g., "last weekend—a quiet celebration with friends"). This taxonomy (or metadata) will exclusively "index" that image for the other participants. Now, consider the same image uploaded to the participant's social network site. Because the site allows tagging of content by other users (folksonomy), the content owner loses exclusive control of the indexing of the image. Now, a "friend" may tag (add metadata to) the image (say, by adding information as to the identity of other participants) or comment on it. Thus, an image that was benign in the water-cooler setting may be re-indexed by other users (e.g., "drunk at medical school reunion;" "so, that's why you missed work"). And, as follows from the discussion above, this re-indexing occurs in a context that allows broadcast to a much larger group consisting of multiple offline but aggregated online social categories.

C. Social Network Privacy and Security Settings

Most social network services provide tools for making data or communications less public. Facebook allows users to choose which information to include in their profiles and limit which users can see that information. MySpace and Twitter similarly allow...
users to control who can see their profile information.\textsuperscript{47} And, of course, appropriately risk-averse users may choose to opt out of the popular social network sites and only post on networks restricted to other licensed physicians.\textsuperscript{48} Indeed, users with multiple profiles tend to create them on different sites. Of social network site users who have multiple profiles, twenty-five percent do so in order to disaggregate their followers, for example by keeping professional relationships on one site and personal ones on another.\textsuperscript{49}

Popular social network sites offer an array of privacy and security technological strategies. For example, by using included “private” modes of communication, users can initiate secure communication without adjusting privacy settings at all. Thus, Facebook, Myspace, and Twitter allow for private messages to be exchanged directly between users,\textsuperscript{50} limiting more sensitive conversations to a specific recipient. Similarly, Facebook allows users to exchange real-time instant messages that can only be viewed temporarily,\textsuperscript{51} lessening concerns about communication records being used later in a negative manner.

Recently distinguishing itself from competitors, Facebook now permits disaggregation of “friends” into multiple categories that can then be set with different permissions.\textsuperscript{52} Utilizing this feature should allow a user to enjoy more relaxed security settings with intimates while benefiting from tightened privacy control for professional contacts.\textsuperscript{53} Simply educating users about these settings can radically reduce exposure of private or semi-private information. For example, the authors of the Florida medical


\textsuperscript{48} See as e.g., Sermo http://www.sermo.com/ , “Our patent-pending technology is the first and only technology to authenticate and credential physicians in real-time. Sermo authenticates each physician when they register. This technology is the key to strictly maintaining a community exclusively for physicians and dramatically improving patient care.” http://www.sermo.com/about/ .

\textsuperscript{49} Pew, Adults and Social Networks, Jan. 14, 2009, at 8.

student and resident survey discussed below\textsuperscript{54} reported that, “telling students to increase their privacy settings on Facebook yielded an 80% reduction in publicly visible accounts.”\textsuperscript{55}

However, such risk management strategies are seriously under-utilized because so few users change the “open” default privacy and security settings on social network sites.\textsuperscript{56} A study conducted by MIT students found that over 70% of the Facebook profiles examined were open to the public.\textsuperscript{57} This is an alarming number when considering that a PEW study found that “47% of internet users look online for information about doctors.”\textsuperscript{58} Further, the MIT study was conducted by using software to automatically examine the information available in user profiles.\textsuperscript{59} Even temporarily unsecured profiles have the potential of being subject to mass data collection, putting users at risk of having their information permanently stored by third-party data aggregators.\textsuperscript{60}

Even proper and consistent use of privacy or security settings has some limitations. Needless to say, such privacy and security settings may, as with any other type of online data storage, be defeated by hackers.\textsuperscript{61} However, social network sites are not subject to the same comprehensive security requirements as HIPAA mandates for healthcare entities.\textsuperscript{62} More importantly, data that is de-identified or rendered pseudonymous may be re-identified if the user has the same profile picture or other demographic data both on one secure and another insecure profile.\textsuperscript{63} Users may also defeat

\textsuperscript{54} Text at note 256.
\textsuperscript{55} Author Reply, L. A. Thompson, MD MS, E. W. Black, MA, K. Dawson, PhD, R. Ferdig, PhD, and N. P. Black, MD, J. GEN INTERN MED 23(12):2156 (2008).
\textsuperscript{57} Harvey Jones and Jose H. Soltren, \textit{Facebook: Threats to Privacy} at § 4.6 (2005).
\textsuperscript{59} 45 CFR Parts 160, 162, and 164.
the purpose of privacy controls purpose by exercising poor judgment in choosing whom to “friend.” For example, a user could have a secured profile but post a comment on another user’s public profile that anyone can see.

Ultimately the solution to many but not all of the issues discussed in this article will themselves be technological. Larry Lessig’s view of ‘code’ or system architecture holds true here, and suggests that features of the architecture of social network sites will “constrain some behavior by making other behavior possible, or impossible.” Changes in the privacy and security settings of Facebook and its fellow travelers will likely be the most efficient “regulation” of these issues, certainly more efficient than case-by-case application of the law of boundaries. As the potential for employment or the availability of health insurance are publicly seen as dependent on more responsible online behavior, so the demand for better architecture will increase, as will its utilization, and the spiral will continue until only outlying scenarios remain.

In parallel to architectural evolution facilitated by code innovation and prompted by market pressures from competitors or consumers, social network services may find themselves subject to low levels of what Anita Allen has in analogous situations termed state “coercion.” Thus, the FTC could exert marginal coercion by, say, opening an investigation into social networking site defaults or, as is happening in Canada, apply additional yet still minimal coercion by demanding specific changes to the sites’ settings.

Whatever the drivers, changes in architecture clearly are foreseeable but are likely to be incremental. The fact that regulation of the physician-patient relationship and the protection of patient information are so entrenched in our health law models (common law, statute, constitutional law, command-control, ethical codes, etc.) makes it unlikely that courts and regulators will wait too long for better “code.”

III. The Legal (and not so Legal) Framework

There are a multitude of emerging legal issues surrounding social network sites and the vast amounts of data contained on them. For example, social network data is of interest to anti-terrorist agencies in much the same way they seek access to email and telephone archives, an Australian court has allowed lawyers to serve notice via Facebook: Threats to Privacy at § 5.10. (2005), http://groups.csail.mit.edu/mac/classes/6.805/student-papers/fall05-papers/facebook.pdf (explaining that their study found 28.7% of Facebook users “friend strangers on occasion”).

Lawrence Lessig, Code (1999) at 89.


See e.g., Office of the Privacy Commissioner of Canada, Facebook needs to improve privacy practices, investigation finds. Privacy Commissioner recommends steps to ensure social networking site better protects the privacy of users and meets the requirements of Canadian privacy legislation, July 16, 2009, http://www.priv.gc.ca/media/nr-c/2009/nr-c-090716_e.cfm.

J Harvey Jones and Jose H. Soltren, Facebook: Threats to Privacy at § 5.10. (2005), http://groups.csail.mit.edu/mac/classes/6.805/student-papers/fall05-papers/facebook.pdf (explaining that their study found 28.7% of Facebook users “friend strangers on occasion”).
book of a default judgment on two borrowers who had defaulted on a loan, and social network postings have come under scrutiny in cases of jurors apparently researching and discussing cases on Twitter and Facebook. Even the status of the very media and data uploaded to social network sites is somewhat uncertain. For example, in February 2009 Facebook changed its terms of use, and for the first time suggested that it had persisting rights in some user-submitted content. Although Facebook changed back to its earlier terms of use, even under the current terms of use some user-uploaded content may persist (when shared with other subscribers or in back-ups) even when deleted by the user.

This article concentrates on just one risk-laden aspect of the use of such networks—the potential for category breakdown between social and healthcare professional uses and its implication for social and professional data. Given that we are concerned primarily with private actors (users of social network sites and those who would view, process, or aggregate user data), the reflexive response is to turn to the “law of boundaries” as the exclusive legal model. Within this concept, the common law of privacy governs social boundaries, while a more complex set of common law, ethical, and regulatory provisions governs professional boundaries. As will be seen, this intuitive response translates into an accurate picture of both the legal structures most likely to be

---

2. Sharing Your Content and Information
You own all of the content and information you post on Facebook, and you can control how we share your content through your privacy and application settings. In order for us to use certain types of content and provide you with Facebook, you agree to the following:

1. For content that is covered by intellectual property rights, like photos and videos (“IP content”), you specifically give us the following permission, subject to your privacy and application settings: you grant us a non-exclusive, transferable, sub-licensable, royalty-free, worldwide license to use any IP content that you post on or in connection with Facebook (“IP License”). This IP License ends when you delete your IP content or your account (except to the extent your content has been shared with others, and they have not deleted it).

2. When you delete IP content, it is deleted in a manner similar to emptying the recycle bin on a computer. However, you understand that removed content may persist in backup copies for a reasonable period of time (but will not be available to others).
applicable, and the legal protection choices of those dissatisfied with treatment of their social network data. But, the law of boundaries does not provide the exclusive options for dealing with category breakdown. Other options present that may prove more or less attractive as these (and related) online interactions develop.

A. Options: Property, Liability, Inalienability, and Soft Law

The conventional wisdom has been that interests in personal health data are protected by liability not property rules. Thus, health information is not directly protected as, for example, an intellectual property system might wall-off some scientific data. Rather, the law of boundaries (HIPAA included) places behavioral limits on those who would obtain or who are entrusted with health information. Even some data protection rules that appear to flirt with property-think, such as rules that exclude regulation of deidentified personal health data, are better understood as liability rules that provide safe harbors for data custodians who behave in certain ways (for example, by deidentifying the data or complying with “limited data set” rules).

There are compelling arguments that property rules are underused in protecting personally identifiable information; for example, Julie Cohen’s dissection of the inapplicability of property as itself conclusory of the property and liberty rhetoric of those who would trade in the data of others. However, of more practical interest in the context of this article is the opening of a “third front,” additional to property or liability constructs; the option of protecting personal information on social networks with some form of inalienability rule.

Stated broadly inalienability denotes non-transferability of an entitlement (herein personally identifiable data) even with (the data subject’s) consent. Here Margaret Jane Radin’s unpacking of inalienability is helpful as is her identification of “market inalienability” that “places some things outside the marketplace but not outside the realm of social intercourse.” With a targeted inalienability regime it is possible to avoid the “on” (property) and “sometimes off” (liability) approaches to tradability in personal information. Specifically, we can impose bright line rules that target specific would-be

---

74 See generally Nicolas P. Terry, Legal Issues Related To Data Access, Pooling, and Use in Healthcare Data in PUBLIC GOOD OR PRIVATE PROPERTY? Ch. 4 (National Institutes of Health, forthcoming 2010).
75 See e.g., HIPAA 45 CFR §160.103 (defining protected health information as that which is “individually identifiable”).
76 See e.g., HIPAA 45 CFR §164.514(a)(3)(i).
uses or users of the data.

Recent developments in health information regulation suggest a growing interest in this targeted approach. For example, the recently-enacted federal Health Information Technology for Economic and Clinical Health Act (HITECH) provides for market inalienability regarding information contained in a patient’s electronic medical record. Similarly, a handful of states have targeted specific uses of prescribing information collected by data aggregators on behalf of pharmaceutical manufacturers desirous of more efficient marketing of their drugs to physicians. The data aggregators initially were successful in arguing that such statutes violated their commercial speech rights. However, the First Circuit Court of Appeals recently validated the regulatory approach when it characterized the limited target prohibition in the New Hampshire statute as restricting conduct, not speech.

Moving forward, inalienability models are useful if we end up concluding that we want to wall-off the social network playground in a less extreme or more targeted manner than by using the law of boundaries. Inalienability rules could prohibit the acquisition of some online information by identified cohorts (for example, health insurers) or particular uses of such data (for example, employment-related decisions).

Finally, in examining the palette of options for dealing with the interaction of social network information and the physician-patient relationship, we must consider “soft law” models of regulation. Soft law is notoriously difficult to define. Previously discussed architectural or “code” approaches to data protection driven by, say, standards bodies or industry associations likely would qualify for the soft law description. However, in the present context the most important sources of non-legal, soft regulation are professional ethics codes; provisions of which will inform the discussion that follows.

Inalienability rules and soft law may not operate in series with liability rules (such as the law of boundaries). Just as common law rules tend to exhibit cycles of on/off switches punctuated by exceptionalism, so highly targeted inalienability or soft law rules may occupy a transitional space while courts determine longer-term entitlements. Equally, narrowly constructed inalienability rules that are consistent with emerging ar-

---

80 Discussed in detail below, text accompanying note 229.
81 HITECH § 13405(d)
82 See e.g., N.H. Rev. Stat. § 318:47-f; 22 M.R.S. § 1711-E.
85 See Dina Epstein, Have I Been Googled?: Character and Fitness in the Age of Google, Facebook, and YouTube (2008) (arguing that the ABA should outlaw consideration of social network data for character and fitness determinations).
chitectural and soft law constructs in, say, being increasingly protective of social net-
work data likely will propel the courts utilizing conventional boundary law mechanisms
towards a similarly protective stance.

B. The Law of Boundaries; Privacy Torts and Breach of Confidence

The Restatement’s black-letter law of “privacy” fails to provide any general or com-
prehensive right of privacy. Rather, the common law of privacy consists of a group of
nominate, discrete, and limited tort causes of action, somewhat unconvincingly bundled
together in the Restatement (Second).88 Most jurisdictions recognize four causes of ac-
tion for invasion of privacy: Intrusion, Public Disclosure (or Publicity) of Private Facts,
False Light, and Appropriation (or exploitation) of another’s name.89 In the context of
this article the Intrusion and Publicity torts are of most importance.90

Both the Intrusion and Publicity torts are collection-centric. That is, they provide for
legal disincentives to the collection or exploitation of private information. The intrusion
tort focuses on the manner of acquisition of the information while the publicity tort fo-
cuses on the content of the information.91 In contrast, the action for breach of confi-
dence recognized in most jurisdictions is disclosure-centric and focuses on the un-
derlying relational source of the information.92

Today courts tend to view the privacy tort as one of public disclosure of embarrass-
ing facts.93 As such it appears to have more in common with the disclosure-centric confi-
dentiality duty than the collection-centric intrusion tort. However, it remains on the
latter, collection-centric side of the line because of its predicate that the defendant ac-
quired private, embarrassing facts about the plaintiff prior to the disclosure. In con-

---

88 Restatement (Second) of Torts § 652 (1965). See e.g., Reid v. Pierce County, 961 P.2d 333 (Wash. 1998)
(adopting § 652).
89 See Loft v. Fuller, 408 So. 2d 619, 622 (Fla. Dist. Ct. App. 4th Dist. 1981); Estate of Berthiaume v. Pratt,
365 A.2d 794 (Me. 1976); Reid v. Pierce County, 961 P.2d 333, 339 (Wash. 1998).
90 Of least importance in the context of this article are the “appropriation” (§ 652C) and “false light” (§
652E) torts. Additionally, not all jurisdictions recognize the “false light” action primarily because it is
somewhat duplicative of the tort of Defamation. Jesus, Inc. v. Rapp, 997 So. 2d 1098 (Fla. 2008), rehear-
tions in recognizing “false light” claim and navigating overlap with defamation). Although not of particular
relevance to the issues discussed herein, it is likely we will see considerable “appropriation” litigation re-
arding social network sites. See e.g., Jim Stanton, Social Media Fraud On the Increase, Digital Commu-
media-fraud-on-the-incr.php (discussing impersonation of media and athletic personalities in twitter
feeds).
91 See Alan Vickery, Note: Breach of Confidence: An Emerging Tort, 82 COLUM. L. REV. 1426, 1441 (1982) (mak-
ing a content-source distinction).
Dec. 27, 2007), at *11 (declining to recognize cause of action for breach of confidence).
964 A.2d 374, 379 (Pa. 2009).
trust, the confidentiality predicate is not one of acquisition by the defendant—rather, the plaintiff delivered the (typically) private information to the defendant in the context of a preexisting, fiduciary relationship.

Based as they are on underlying, preexisting relationships, breach of confidence actions are heavily dependent on context and the properties of that underlying relationship. In the context of the physician-patient relationship and the data entrusted in that context, the breach of confidence actions discussed below are variously based on responsibilities imposed by licensing statutes, the physician’s evidentiary privilege, common law principles of trust, the Hippocratic oath, and general principles of medical ethics.95

1. Intrusion Upon Seclusion

The Restatement (Second) describes the “Intrusion Upon Seclusion” tort as follows:

One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person.96

Today, courts require the satisfaction of four elements: (1) an unauthorized intrusion or prying into plaintiff’s seclusion; (2) the intrusion is highly offensive or objectionable to a reasonable person; (3) the matter upon which the intrusion occurs must be private; and (4) the intrusion causes anguish and suffering.97

The intrusion tort originally required a literal, physical intrusion; this is no longer the case. Courts now tend to look less at the physicality of the defendant’s action and more at the level of its offensiveness.98 The foundation of the action remains an “intentional and unwarranted acquisition by the defendant.”99

A “wrongful intrusion may occur in a public place, so long as the thing into which

96 Restatement (Second) of Torts § 652B (1965). See also § 652B Comments:
   a. The form of invasion of privacy covered by this Section does not depend upon any publicity given to the person whose interest is invaded or to his affairs. It consists solely of an intentional interference with his interest in solitude or seclusion, either as to his person or as to his private affairs or concerns, of a kind that would be highly offensive to a reasonable man.
   b. The invasion may be by … some other form of investigation or examination into his private concerns, as by opening his private and personal mail, searching his safe or his wallet, examining his private bank account…
there is intrusion or prying is entitled to be private.” However, “generally, the observation of another person’s activities, when that other person is exposed to the public view, is not actionable.” Thus training a surveillance camera on the outside of a house likely will not be an intrusion. However, observing people through holes poked in the ceiling of a restroom, or by use of a camera installed in a medical examination room clearly satisfy the element.

As the courts’ understanding of an actionable intrusion has become more existential, so too has their approach become more nuanced. In the words of one court:

Assuming that the matter is entitled to be private, then the court will consider two primary factors in determining whether an intrusion is actionable: (1) the means used, and (2) the defendant’s purpose for obtaining the information.

In general (and contrasting sharply with other boundary torts), “[i]ntrusion into solitude appears to be based on the manner in which a defendant obtains information, and not what a defendant later does with the information.”

2. Public Disclosure of Private Facts

The “publicity” tort, targeting those who give “publicity to a matter concerning the private life” of the plaintiff, applies to “[a]ny who gives publicity to a matter concerning the private life of another” if the data “(a) would be highly offensive to a reasonable person, and (b) is not of legitimate concern to the public.” Modern courts state a granular version of the doctrine as requiring:

(1) the fact or facts disclosed must be private in nature; (2) the disclosure must be made to the public; (3) the disclosure must be one which would be highly offensive to a reasonable person; (4) the fact or facts disclosed cannot be of legitimate concern to the public; and (5) the defendant acted with reckless disregard of the private nature of the fact or facts disclosed.

A key distinction between the intrusion and publicity causes of action is that while the former “requires no showing of publication or publicity,” the publicity action rotates...
around the public disclosure of private facts.\textsuperscript{111}

\section*{3. Breach of Confidence}

The privacy torts closely resemble intentional torts such as "outrage,"\textsuperscript{112} in that they rotate around intentional interferences\textsuperscript{113} that are "highly offensive to a reasonable person."\textsuperscript{114} In contrast, the breach of confidence tort is essentially a strict liability action,\textsuperscript{115} as befits a tort claim that had its roots in implied contract and fiduciary duties.\textsuperscript{116}

Confidentiality, or rather the tort of "breach of confidence," is disclosure-centric. The breach of confidence applies only to those who have been entrusted with information in confidence.\textsuperscript{117} Accordingly:

The (fiduciary or confidential) relationship arises when one person reposes special trust and confidence in another person and that other person - the fiduciary - undertakes to assume responsibility for the affairs of the other party. The person upon whom the trust and confidence is imposed is under a duty to act for and to give advice for the benefit of the other person on matters within the scope of the relationship. Fiduciary duties are the highest standard of duty imposed by law.\textsuperscript{118}

It follows that "[o]nly one who holds information in confidence can be charged with a breach of confidence,"\textsuperscript{119} while "an act [that] qualifies as a tortious invasion of privacy ... theoretically could be committed by anyone."\textsuperscript{120} The converse is true; if information that is not secret or private is entrusted in confidence, its subsequent disclosure may be actionable.\textsuperscript{121} While there can be overlap "neither of the torts of invasion of privacy nor breach of confidentiality is entirely subsumed within the other."\textsuperscript{122}

The breach of confidence tort not only is a stricter form of liability than privacy

theories, but also eschews the defensive arguments available in the latter. For example, a “defendant is not released from an obligation of confidence merely because the information learned constitutes a matter of legitimate public interest.”

C. Privacy Expectations & Social Networks

Obviously privacy policies do not protect social network subscribers from legal process. Increasingly, and as happened with email, social network subscribers’ “private” profile pages are drawn into public processes through subpoena or discovery. For example, there have been media reports of prosecutors using photographs posted on defendants’ social network sites to bolster their arguments in sentencing hearings. Indeed, a growing number of cases involve discovery or related procedural requests by defendants. Representative fact-patterns include workplace sexual harassment claims (where the defendant argues that the plaintiff consensually engaged in similar behaviors online) and any number of cases where the defense seeks to make an issue out of the social network subscriber’s emotional state.

In such cases the exact legal status of social network content vis-à-vis user expectations tends to be obscured by proceedings that depend in large part on highly individualized facts and trial court discretion. Only occasionally have courts dealt directly with a social network user’s expectations of those who can see their posts, or the more complex legal question of the user’s privacy expectations.

A.B. v. State concerned a juvenile who posted a vulgar tirade against her ex-middle

124 See e.g., Facebook’s Privacy Policy that notes:
We may be required to disclose user information pursuant to lawful requests, such as subpoenas or court orders, or in compliance with applicable laws. We do not reveal information until we have a good faith belief that an information request by law enforcement or private litigants meets applicable legal standards.
http://www.facebook.com/policy.php
129 See e.g., Beye v. Horizon and Foley v. Horizon, discussed in Mary Pat Gallagher, MySpace, Facebook Pages Called Key to Dispute Over Insurance Coverage for Eating Disorders, NEW JERSEY L. J., Feb 1, 2008, http://www.law.com/jsp/article.jsp?id=1201779829458 (federal court actions against health insurer for denial of coverage for anorexia or bulimia in which defendant argued that access to social network pages could assist in a defense conditions were emotionally not biologically caused).
130 885 N.E.2d 1123 (Ind. 2008).
school principal on a MySpace page. That page was on a profile falsified as the principal’s, but actually created by one of the defendant’s friends.\textsuperscript{131} A total of 26 “friends” including the defendant were given access to the fake profile.\textsuperscript{132} At trial the defendant was adjudicated a delinquent child on the basis that, if she had been an adult at the time of the crime, she would have committed the statutory offense of harassment.\textsuperscript{133} The requisite intent for the harassment offense in question included “a subjective expectation that the offending conduct will likely come to the attention of the person targeted for the harassment.”\textsuperscript{134} Given the sparse record, the prosecution’s reasonable doubt burden, and a lack of any independent evidence as to the workings of the social network site, the court reversed the adjudication.\textsuperscript{135} Specifically, the court determined that there was no probative evidence that the defendant, who posted to a limited group of friends rather than the public, had the requisite expectation that the act would come to the principal’s intention.\textsuperscript{136}

In Moreno v. Hanford Sentinel, Inc.,\textsuperscript{137} a college student posted comments critical of her hometown on her MySpace site. Although she removed the posting six days later, the post had already been copied to her hometown’s newspaper for republication.\textsuperscript{138} She sued the newspaper and her high school principal (who had transmitted the posting to a reporter) for, \textit{inter alia}, breach of privacy.\textsuperscript{139} Citing Hill v. National Collegiate Athletic Assn., the California Supreme Court’s most recent guide, the court noted that such a claim “is not so much one of total secrecy as it is of the right to define one’s circle of intimacy—to choose who shall see beneath the quotidian mask.”\textsuperscript{140} The Moreno court concluded:

\textit{[T]he [plaintiff] publicized her opinions … by posting …on MySpace.com, a hugely popular Internet site. [Her] affirmative act made her article available to any person with a computer and thus opened it to the public eye. Under

\begin{flushleft}
\textsuperscript{131} Id. at 1225.
\textsuperscript{132} Id.
\textsuperscript{133} 885 N.E.2d at 1223-25.
\textsuperscript{135} Id. at 1228.
\textsuperscript{136} 885 N.E.2d at 1227. The court seemed less sure about how to deal with another posting by the defendant on a different, public MySpace profile page, but ultimately found the evidence wanting as to intent. Id. at 1227-28.
\textsuperscript{137} 172 Cal. App. 4th 1125 (5th Dist., 2009).
\textsuperscript{138} Id. at 1228.
\textsuperscript{139} Id. at 1229.
\textsuperscript{140} (1994) 7 Cal. 4th 1, 25. Hill also analyzed the privacy tort rights as follows:

\begin{itemize}
  \item Each of the four categories of common law invasion of privacy identifies a distinct interest associated with an individual’s control of the process or products of his or her personal life.
  \item To the extent there is a common denominator among them, it appears to be improper interference (usually by means of observation or communication) with aspects of life consigned to the realm of the “personal and confidential” by strong and widely shared social norms.
\end{itemize}
\end{flushleft}
these circumstances, no reasonable person would have had an expectation of privacy regarding the published material.\footnote{141} The opinion does not state whether the plaintiff had set her MySpace privacy settings to restrict access to her site to her approved “friends.” As it stands the opinion seems to suggest that simply posting to a social network site defeats the expectation of privacy; a position that is challenged below.\footnote{142}

\section*{D. Privacy and Confidentiality in Healthcare}

The privacy and confidentiality rules applied to healthcare providers and to some patient information are both more complex and granular. At common law, the collection-centric privacy tort is represented by a relatively small collection of cases that suggest healthcare provider liability will be restricted to a narrow range of outlying fact situations. Such a state is unsurprising given that the privacy torts lack any unifying concept and have failed to develop robust, plaintiff-friendly doctrine.

Consider, for example, the classic case of \textit{Knight v. Penobscot Bay Med. Ctr.}\footnote{143} A nurse’s husband arrived at a hospital to pick up his wife.\footnote{144} To give him something to do while he waited, the husband was gowned and permitted to observe a stranger’s labor and delivery.\footnote{145} Notwithstanding the rather obvious nature of this intrusion, the plaintiff’s cause of action failed because there was no evidence that the nurse’s husband had intended the intrusion into the patient’s seclusion.\footnote{146}

Similar limitations that are instructive on the application of the privacy torts to social network scenarios derive from the torts’ offensiveness and privacy expectations limitations. Take, for example, \textit{Adamski v. Johnson},\footnote{147} a case that involved breach of privacy (intrusion and publicity) allegations by the plaintiff against her employer. Plaintiff provided her employer with notice that she would be undergoing surgery, but when asked she refused to supply additional information about the surgery.\footnote{148} Allegedly, her supervisor applied pressure to her co-employees and acquired that information.\footnote{149} The defendants’ apparently intentional conduct notwithstanding, the court granted defendants’ demurrer.\footnote{150} First, the court did not view the disclosed information regarding the nature of the surgery as either an intrusion or public disclosure of private facts that

\footnote{141} 172 Cal. App. 4th at 1130.
\footnote{142} Text accompanying note 315.
\footnote{143} 420 A.2d 915 (Me. 1980).
\footnote{144} Id. at 916.
\footnote{145} Id. at 917.
\footnote{148} Id. at 70.
\footnote{149} Id. at 71.
\footnote{150} Id.}
could be "highly offensive" to a reasonable person.  Second, the plaintiff's inchoate allegation that her supervisor relayed the information to others was dismissed on the basis that it did not allege facts to suggest that the disclosure went beyond a single person or small group of persons.  Third, the plaintiff's own disclosure of the nature of the surgery to a small group of co-workers reinforced the defense position that the intrusion was not offensive and rendered the publicity claim untenable by eliminating her expectation of privacy.

Notwithstanding these limitations inherent in the common law doctrines, there is a considerable body of case law that applies privacy doctrine with some rigor to medical fact patterns and suggests some legal jeopardy for medical professionals posting or micro-blogging information about their patients. As noted as early as 1942 by the Supreme Court of Missouri, "if there is any right of privacy at all, it should include the right to obtain medical treatment at home or in a hospital for an individual personal condition (at least if it is not contagious or dangerous to others) without personal publicity." As more recently stated by a District Court in Illinois, "[t]here are few things in life that are more private than medical treatments and/or examinations."

1. Intrusion Actions

_Estate of Berthiaume v. Pratt_ concerned two series of photographs taken of a patient suffering from cancer of the larynx. The first series was taken during the patient's treatment and apparently with his consent. A second series was taken as the patient was dying and there was evidence that the patient objected to the taking of this second set of photographs. The court reversed the defendant's directed verdict and held that this intrusion claim should have been submitted to the jury. Although the court recognized "the benefit to the science of medicine which comes from the making of photographs of the treatment and of medical abnormalities found in patients," this could not be done without the subject's consent.

_Sтраттан v. Кrywka_ concerned a plaintiff involved in an automobile accident. She was taking Prozac and on the night of the accident consumed alcohol and marijuana. With the consent of emergency services and the local hospital, a documentary crew was riding

---

151 Id. at 74.
152 Id. at 76.
153 A similar result was reached in Fletcher v. Price Chopper Foods of Trumann, Inc., 220 F.3d 871, 878 (8th Cir. Ark. 2000) (plaintiff lost expectation of privacy when she shared information about a staph infection with co-workers).
154 Barber v. Time, Inc., 159 S.W.2d 291, 295 (Mo. 1942).
156 365 A.2d 792 (Me 1976).
157 Id. at 793.
158 Id. at 792.
159 Id. at 795.
160 Id.
with the paramedics who treated the patient at the scene of the accident and transported her to the emergency room. Plaintiff refused to sign any consent to the filming. In subsequent broadcasts plaintiff’s face was digitally obscured. However, she was referred to by her first name and her name and address were visible on a report shown in the video. A physician could be heard referring to her as “[n]o allergies, on Prozac.”\textsuperscript{161} Given that “defendants filmed plaintiff in the emergency room after she was presented with and explicitly refused to sign the informed consent release,”\textsuperscript{162} the court held that her intrusion allegation should have been presented to the jury.\textsuperscript{163}

Both Berthiaume and Stratton reaffirm the collection-centric nature of the Intrusion action. However, both cases concern the judicial protection of overtly physical spaces and tell us little about the resolution of potential claims involving intrusion into a pseudo-secluded space such as a Facebook profile.

2. Publicity Actions

Whether information is “private” depends in part on the type of information and the extent that the subject keeps the information from the public. Thus, “sexual relations … are normally entirely private matters, as are … many unpleasant or disgraceful or humiliating illnesses, most intimate personal letters, (and) most details of a man’s life in his home….\textsuperscript{164} Indeed, “[m]atters concerning a person’s medical treatment or condition are also generally considered private.”\textsuperscript{165} Just as the taking of photographs can constitute an intrusion,\textsuperscript{166} so the publicity tort may apply to their distribution. For example, one court opined, “[w]e fail to see how autopsy photographs of the Plaintiffs’ deceased relatives do not constitute intimate details of the Plaintiffs’ lives or are not facts Plaintiffs do not wish exposed ‘before the public gaze.’”\textsuperscript{167} On the other hand, “there is no liability for giving further publicity to what the plaintiff himself leaves open to the public eye.”\textsuperscript{168}

The core component of the publicity tort is, not surprisingly, that the defendant gave publicity to this private information. The relevant Restatement (Second) comment provides:

it is not an invasion of the right of privacy, within the rule stated in this Section, to communicate a fact concerning the plaintiff’s private life to a single person or even to a small group of persons. On the other hand, any publication in a newspaper or a magazine, even of small circulation, or in a handbill

\textsuperscript{162}Id. at 20.
\textsuperscript{164}Restatement (Second) of Torts § 652D, com. b.
\textsuperscript{166}Text at note 158.
\textsuperscript{167}Reid v. Pierce County, 961 P.2d 333, 341 (Wash. 1998).
\textsuperscript{168}Restatement (Second) of Torts § 652D, com. b.
distributed to a large number of persons, or any broadcast over the radio, or statement made in an address to a large audience, is sufficient to give publicity within the meaning of the term as it is used in this Section. The distinction, in other words, is one between private and public communication.  

In this context, *Vassiliades v. Garfinckel’s* is instructive.  

A patient brought an action against her plastic surgeon for invasion of privacy (Publicity) after the surgeon used “before” and “after” photographs of her (taken with her consent) in promotional events at a department store and on television. Evidence had been offered at trial by the plaintiff that “after agonizing over losing her youthful appearance and contemplating plastic surgery for many years, she underwent plastic surgery and kept her surgery secret, telling only family and very intimate friends.”  

For the court, there was no touchstone regarding who had seen the photographs or even whether her name had been published. Rather the “nature of the publicity ensured that it would reach the public.”  

Compare *Robert C. Ozer, P.C. v. Borquez*. The plaintiff’s partner was diagnosed with AIDS and the plaintiff himself was advised to take an HIV test. Asking for confidence the plaintiff, an associate at a law firm, told his law firm president that he was gay, that he needed to be tested, and wished for some help covering a previously scheduled deposition. One-week later the plaintiff was terminated but not before he discovered that the information had been shared with everyone in the law firm. The court reversed a jury verdict in the plaintiff’s favor on a “publicity” count because of a defective jury instruction: the trial court had required only that the private information be “published” to another. As the Supreme Court of Colorado concluded, “the public disclosure requirement renders [defendant] liable for … invasion of privacy claim only if [defendant] disclosed [plaintiff’s] situation to a large number of persons or the general public.”  

As discussed below *Vassiliades* and *Ozer* are not at odds with each other. Rather, modern courts recognize a more granular interpretation of the publicity tort whereby the “publicity” can occur either through “private” channels (thus triggering an additional requirement of a considerable number of recipients) or through a “public” channel (anything from a sign in a shop window to a television) broadcast (in which case there is no additional numerical touchstone).  

Given that the action rotates around private facts being made public, plaintiffs will

---

169 Restatement (Second) of Torts § 652D, com. a.
171 492 A.2d at 588.
172 Id.
174 Id. at 373.
175 Id. at 374.
176 Id.
177 Id. at 379.
178 940 P.2d at 379.
179 See discussion at text accompanying note 295.
have weaker cases when there has been some level of self-disclosure. *Stratton v. Krywko*, the television documentary case discussed above, was close to the line. The defendants had successfully argued in their motion for summary judgment that the information disclosed about the plaintiff (such as her face, x-ray/cat scan data, status, prognosis, and Prozac prescription) was already public. The appellate court agreed with regard to many of the items (for example, a public street accident, the police report of the accident) while others (e.g., scans) were not specifically identified during the broadcasts as hers. However, the court considered that there was an issue of triable fact as to whether her Prozac prescription was known to “everybody” as argued by defendants or known to only a “select number of close friends and family.” As the court recognized “[p]laintiff’s argument has merit. Disclosing a fact to a small number of confidants does not equate to making the information public.”

Another issue that arises in publicity cases is whether the publicity reaches the “highly offensive” threshold. This question of offensiveness to a reasonable person is an issue of fact for the jury. For example, the court in *Vassiliades* would not substitute its own views for a jury determination that the publication of “before” and “after” photographs met this test.

The publicity tort can be defeated in the case of the qualified “legitimate public interest in the publication,” either at common law or when the First Amendment is implicated. Notwithstanding, when balancing out these interests, courts tend to favor the individual’s right to privacy: “The line is to be drawn when the publicity ceases to be the giving of information to which the public is entitled, and becomes a morbid and sensational prying into private lives for its own sake, with which a reasonable member of the public, with decent standards, would say that he had no concern.”

*Gilbert v. Medical Economics Co.* concerned an article in defendant’s magazine that discussed incidents of alleged malpractice committed by the plaintiff anesthesiologist. The article discussed the plaintiff’s history of psychiatric and related personal problems in making the argument that there had been a breakdown in the regulatory system. The court affirmed the defendant’s summary judgment on the application of the defense noting “the legitimate public interest of warning potential future patients, as well as

---

180 Text at note 161.
181 Id. at *14.
183 Id.
184 492 A.2d at 588.
185 Id. at 588-89. See also *Gilbert v. Medical Economics Co.*, 665 F.2d 305 (10th Cir. Colo. 1981), *Robert C. Ozer, P.C. v. Borquez*, 940 P.2d 371 (Colo. 1997) (discussing 1st Amendment’s applicability). See also *Fisher v. Dep’t of Health*, 106 P.3d 836, 840 (Wash. Ct. App. 2005) (“the government may have had no legitimate interest in the dissemination of this private information sufficient to outweigh Ms. Fisher’s protected privacy interest. But she must show that the extent of the dissemination outweighed her own privacy interest”).
186 Restatement (2nd) of Torts, § 652D, com. h.
187 665 F.2d 305 (10th Cir. Colo. 1981).
surgeons and hospitals, of the risks they might encounter in being treated by or in employing the plaintiff.\textsuperscript{188}

The most difficult issue in these public interest cases is the assessment of the value of the specific identification. Consider again Stratton v. Krywko, where the defendants had persuaded the trial court that the First Amendment protected their ‘Night in the E.R.’ documentary as newsworthy or educational.\textsuperscript{189} The court reaffirmed the duality of this inquiry: “not only must the overall subject-matter be newsworthy, but also the particular facts [regarding the plaintiff] revealed.”\textsuperscript{190} On these facts, the court considered summary adjudication to be improper.\textsuperscript{191} When dealing with this issue the courts, as noted in Vassilades,\textsuperscript{192} seek a “logical nexus” between the legitimate public interest and the particular publicity given to the plaintiff’s private information.\textsuperscript{193}

3. Confidentiality Actions

As discussed above, the tort action for breach of confidence is disclosure-centric and dependent on context. There is also a chronology at play (and as persuasively argued by Leslie Francis, it is a chronology not a prioritization\textsuperscript{194}); a patient exercises this right of privacy when he or she chooses to provide information to a physician: “[i]f it were otherwise, patients would be reluctant to freely disclose their symptoms and conditions to their physicians in order to receive proper treatment.”\textsuperscript{195} That information then ceases to be private vis-à-vis the physician. Thereafter, dissemination of that information by the physician is limited by the requirement of confidence.\textsuperscript{196}

One of the fiduciary duties that a physician assumes when he or she undertakes to treat a patient is the duty to refrain from disclosing a patient’s confidential health information unless the patient expressly or impliedly consents or unless the law requires or permits disclosure.\textsuperscript{197}

The modern trend is to apply a tort-based breach of confidence action regarding unauthorized disclosure of medical information.\textsuperscript{198} For example, in Biddle v. Warren Gen. Hosp., the court recognized both healthcare provider liability for either “unprivileged disclosure to a third party of nonpublic medical information that a physician or hospital

\textsuperscript{188} 665 F.2d at 309.
\textsuperscript{191} Id.
\textsuperscript{192} 492 A.2d 580, 585 (D.C. 1985).
\textsuperscript{193} Id at 589-90 (citations omitted).
\textsuperscript{195} Overstreet v. TRW Commer. Steering Div., 256 S.W.3d 626, 642 (Tenn. 2008) (citations omitted).
\textsuperscript{197} Overstreet v. TRW Commer. Steering Div., 256 S.W.3d 626, 642 (Tenn. 2008) (citations omitted).
has learned within a physician-patient relationship or third party liability for "inducing the unauthorized, unprivileged disclosure of nonpublic medical information." In enforcing the duty of confidentiality regarding medical information courts are particularly protective of medical records. For example, in Hageman v. Southwest Gen. Health Ctr., the Supreme Court of Ohio reaffirmed its holding in Biddle and held a lawyer liable for breach of confidence when she passed medical records lawfully obtained in a divorce case to a prosecutor in a related matter.

Although there is no public interest defense to breach of confidence, "a physician or hospital is privileged to disclose otherwise confidential medical information in those special situations where disclosure is made in accordance with a statutory mandate or common-law duty, or where disclosure is necessary to protect or further a countervailing interest which outweighs the patient's interest in confidentiality." As with the statutory and regulatory confidentiality codes discussed below, breach of confidentiality actions can be met by defensive arguments that the disclosure was compelled by law, is in the best interest of the patient or others, or the patient has given express or implied consent to the disclosure.

E. Ethical Restraints

Just as system architecture creates a soft law alternative to boundary law or governmental coercion, so the existing ethical boundaries that hover over the physician-patient relationship create a soft law approach to modulating the behaviors of some social network actors.

Basic medical professional ethics structures map quite well to the common law confidentiality and privacy restraints. Thus the AMA Code combines its disclosure-centric requirement of confidence (“The physician should not reveal confidential information without the express consent of the patient”) with the principle’s instrumental justification (“The patient should feel free to make a full disclosure of information to the physician in order that the physician may most effectively provide needed services”). Similarly, the AMA’s approach to collection-centric rules includes an “intrusion”-like

200 Id. et para. 3.
201 893 N.E.2d 153 (Ohio 2008).
203 Note 123.
204 715 N.E.2d at 156.
206 Id.
207 Snavely v. AMISUB of South Carolina, Inc., 665 S.E.2d 222 (S.C. Ct. App. 2008) [note, cert has been granted in this case].
privacy principle demanding protection of patient privacy as it relates to physical [privacy] "which focuses on individuals and their personal spaces."\(^{209}\) However, the ethical rules also extend to associational ("family or other intimate relations"), informational, ("specific personal data") and decisional privacy ("personal choices").\(^ {210}\)

As discussed above, the legal domain’s case-by-case approach to physician-patient privacy has added few bright line rules to the basic seclusion-intrusion or related mandates. In contrast, the AMA principles do bright line some specific fact-patterns.

Thus, physicians who participate in “interactive online sites that offer email communication” are expected to adhere to the AMA’s guidelines on email.\(^{211}\) It might seem that these guidelines would apply only to the email-like features grafted on to social network sites. However, the AMA opinion could be interpreted to provide guidelines for broader physician participation online and so prohibit the establishment of a physician-patient relationship through an online social network. Further, if a physician-patient relationship already existed such guidelines would require informed consent as to the limitations and risks associated with social network communication, and demand a regard for privacy and confidentiality that may be unattainable in the online social network context.\(^ {212}\)

The AMA ethical guidelines specifically address both contemporaneous and recorded observation of physician-patient interactions, scenarios that may point to the correct approach to social network “broadcasts” such as Facebook posts or Twitter streams. For example, the ethical approach to “outside observers”\(^ {213}\) requires their prior agreement to confidentiality and their presence is conditioned on “the patient’s explicit agreement.”\(^ {214}\) Similarly, with regard to filming and broadcasting encounters, the “educational objective can be achieved ethically by filming only patients who can consent.”\(^ {215}\) Such consent must be obtained for both the filming and subsequent broadcasting.\(^ {216}\) Any such consent must be informed and thus is predicated on:

[A]n explanation of the educational purpose of film, potential benefits and harms (such as breaches of privacy and confidentiality), as well as a clear statement that participation in filming is voluntary and that the decision will not affect the medical care the patient receives.\(^ {217}\)

\(^{209}\) Id. § 5.059 - Privacy in the Context of Health Care.
\(^ {210}\) Id. § 5.059 - Privacy in the Context of Health Care.
\(^ {211}\) Id. § 5.027(3) – Use of health-Related Online Sites.
\(^ {213}\) “[I]ndividuals who are present during patient-physician encounters and are neither members of a health care team nor enrolled in an educational program for health professionals…” Id. § 5.0591 - Patient Privacy and Outside Observers to the Clinical Encounter.
\(^ {214}\) Id.
\(^ {215}\) Id. § 5.045(1)(2) - Filming Patients in Health Care Settings.
\(^ {216}\) Id.
\(^ {217}\) Id.
Furthermore, the guidelines assume that the filming and broadcast will be limited to healthcare professionals and their students. If any broader audience is contemplated, that must be the subject of an additional, explicit consent.\textsuperscript{218}

The framing of both the provisions on outside observers and filming are sufficiently analogous to Internet broadcasting through social network sites that the additional considerations regarding confidentiality and informed consent are significant. First, the AMA notes that, "\textquote[AMA. § 5.046(2)]{Physicians should avoid situations in which an outside observer's presence may negatively influence the medical interaction and compromise care.} Second, "\textquote[AMA. § 5.0591]{Physicians should be aware that filming may affect patient behavior during a clinical encounter. The patient should be given ample opportunity to discuss concerns about the film, before and after filming, and a decision to withdraw consent must be respected.} Third, the ethical rules that acknowledge the requirement for explicit consent are based on the recognition that "\textquote[AMA. § 5.045(2)]{Filming cannot benefit a patient medically and may cause harm.}"

\section*{F. HIPAA and Related Regulatory Models}

Although reasonably well-developed areas of law by the late 1990s, the breach of confidence tort and related state statutes\textsuperscript{222} were deemed inadequate to meet the needs of electronic, interoperable billing and records systems. Starting in 2000, therefore, the breach of confidence tort has been supplemented by HIPAA, a federal confidentiality code (albeit one that is mislabeled as dealing with "privacy").\textsuperscript{223}

Today, the HIPAA code is regarded as the most important source of regulation regarding disclosures of patient information by healthcare providers.\textsuperscript{224} It is not the exclusive source because HIPAA is quite limited in its reach\textsuperscript{225} and only partially preempts state confidentiality laws.\textsuperscript{226} Much of the HIPAA regulatory framework is not directed at protecting patient information but creating the "exceptional" processes by which such data may be disseminated (such as patient consent) or creating broad safe harbors for public health, judicial, and regulatory institutions.\textsuperscript{227} Additionally, there have been strong critiques of the Office of Civil Rights in its approach to enforcing the regulations.\textsuperscript{228}
Some of the complaints about HIPAA’s limitations should be addressed as a result of the Health Information Technology for Economic and Clinical Health Act” (HITECH), Subtitle D, (part of the American Recovery and Reinvestment Act of 2009). For example, ‘Business Associates’ are no longer indirectly regulated through terms in their contracts with ‘Covered Entities’ but are directly subject to the HIPAA code, including its penalties. HITECH seeks to respond to criticisms about HIPAA’s lack of an educative goal, requiring regulations on educating health providers and an initiative to “enhance public transparency regarding the uses of protected health information.” The legislation requires new regulations to strengthen the proportionality (“minimum necessary” under HIPAA) of disclosures and strengthened restrictions on the use of protected health information for marketing purposes. Enforcement should improve because of both tighter definitions of breaches of the code and additional enforcement through state attorneys general. Although there is still no private right of action, there will be a system designed to distribute a percentage of civil penalties or settlements collected from providers to injured patients.

Notwithstanding, the HIPAA approach to preemption, the HIPAA “floor,” continues. Further, the exact changes to the confidentiality code will depend on regulations made pursuant to the enabling legislation included in HITECH.

While the HIPAA code and this forthcoming “version 2.0” are relevant to the regulation of the social network fact patterns discussed in this article, they are of less importance than in traditional, offline healthcare “boundary” scenarios. Running a Twitter feed from inside a hospital or physician blog posts that identify patients would seem to implicate HIPAA’s “covered entity” requirements as far as confidentiality and consent. However, HIPAA still only applies to data entrusted to and subsequently disclosed by healthcare providers. Thus, patient health information that is posted to a social network site by someone other than a covered entity (e.g., by the patient) will not trigger HIPAA.

Perhaps the most important limitation of HIPAA relevant to this article is that the federal code does not create boundaries as to the collection of patient information (e.g., by insurers, employers or even physicians surfing patient profiles), but only its disclosure. As a result, most of the “boundary” analysis that follows will rotate around common law

theories of liability.

IV. Setting Boundaries for Physicians and Patients

Patients and their healthcare providers are robust users of global and enterprise wide networks. However, the two groups seldom intentionally interact using such tools, notwithstanding governmental and healthcare institutions interest in promoting online interactions such as researching efficient healthcare interventions or sharing electronic medical records. More than 61 percent of U.S. adults search for health information online. Sustained growth in patient enthusiasm for online interactions notwithstanding, many physicians still view direct contact with patients via email as time-consuming tasks best left to staff or creating unacceptable time pressures during consultations, and the AMA remains concerned that email contact will damage the traditional framework of the physician-patient relationship.

To this dystopian online world of physicians and patients now must be added category-blurring behavior by both cohorts: physicians intending to blog or “tweet” to other physicians but reaching a far broader audience; patients exposing medical or genetic signals in apparently private interactions online. Physicians but reaching a far broader audience; patients exposing medical or genetic information online.

Meanwhile regulators and prosecutors take the position that online practice encourages opportunistic online relationships designed to encourage the illegal distribution of prescription drugs.

To this dystopian online world of physicians and patients now must be added category-blurring behavior by both cohorts: physicians intending to blog or “tweet” to other physicians but reaching a far broader audience; patients exposing medical or genetic signals in apparently private Facebook posts; physicians disclosing sufficient personal information on their profile pages to concern a patient or raise a red flag during a pre-

---


245 Prescriptions sans Frontières, supra note 241, at 227.


248 Prescriptions sans Frontières, supra note 241, at 243-45.
employment background check; and, physicians entering perhaps unintended relationships with a small number of the undifferentiated cohorts they meet online.

This section seeks to identify some of the “pinch points” that could lead to legal exposure for healthcare providers or an array of surprises for patients.

A. Physicians’ Social Information Online

“Search” is omnipresent as both a personal and professional tool. We can “Google” our friends or colleagues and increasingly may view it as unprofessional to take a meeting with someone un-researched.

In fact, 35 percent of U.S. adults have used the Internet to search for information about physicians or other healthcare professionals.249 A slightly smaller group (28 percent) searches for information about institutional providers.250 There is a robust correlation between the adults that search for information online and those who use social network sites; some 39 percent of the former cohort use social network sites.251 Emerging consumer-driven healthcare models suggest that patients should research their potential providers.

There are innumerable, searchable databases regarding regulatory proceedings or litigation with adverse results for physicians. These include The National Practitioner Data Bank,252 the Federation Physician Data Center,253 and resources maintained by state medical boards.254 However, these databases are not always complete (although the reach of the NPDB may be expanding255) and seldom will document social behavior.

In 2008, Thompson and colleagues evaluated the Facebook profiles of University of Florida medical students and residents. 44.5 percent of medical students had a Facebook account, but only 37.5 percent of profiles were made private. The study found that, “Use is more common among students, and most chose to keep their profiles open to the public.” The study found that many of these accounts included personal information “that is not usually disclosed in a doctor–patient relationship.”256 A random sub-sample of such studied sites disclosed; “content that could be interpreted negatively,” such as

---

249 Social Life of Health Information, note 243, at 35.
250 Social Life of Health Information, note 243, at 46.
251 Social Life of Health Information, note 243, at 15.
253 http://www.fsmb.org/m_fpdc.html
254 See e.g., the Virginia Board of Medicine’s Practitioner Information Website, http://www.vahealthprovider.com/.
excess alcohol consumption and foul language.\textsuperscript{257}

As discussed below employers routinely search the social network sites of applicants and employees even though this practice is not without legal risk.\textsuperscript{258} Such disincentives notwithstanding, in the wake of high-profile hiring scandals the case can be made that no hospital or system should make a professional appointment without first performing a detailed background check using all available search tools: including searches of social network sites. Recall, for example, the data available about some of the Florida medical.\textsuperscript{259} Further, a social network profile might contain postings, uploaded and tagged data, or membership in online groups that could signal anything from substance abuse to attitudes about race or gender.

In the healthcare domain this background-checking issue is of increasing importance because of the rise of so-called 'negligent credentialing' suits brought by a patient against a health care facility allegedly injured as a result of the acts or omissions of a facility-credentialed physician. In Larson v. Wasemiller, the Supreme Court of Minnesota noted:

\begin{quote}
Given our previous recognition of a hospital’s duty of care to protect its patients from harm by third persons and of the analogous tort of negligent hiring, and given the general acceptance in the common law of the tort of negligent selection of an independent contractor, as recognized by the Restatement of Torts, we conclude that the tort of negligent credentialing is inherent in and the natural extension of well-established common law rights.\textsuperscript{260}
\end{quote}

The Larson court’s 2007 opinion identified 27 states that have recognized some form of the cause of action,\textsuperscript{261} notwithstanding the difficult causation issues such suits pose.\textsuperscript{262}

While Larson recognized an action by the patient against the credentialing hospital, an important, additional legal implication was discussed in Kadlec Med. Ctr. v. Lakeview Anesthesia Assocs.\textsuperscript{263} A patient in the plaintiff’s medical center emerged from routine tubal ligation surgery in a permanent vegetative state. The medical center settled a claim based on its respondeat superior for the alleged negligence of a drug-addicted anesthesiologist. The medical center and its malpractice carrier then filed suit against the medical group where the anesthesiologist had previously practiced and the hospital where he worked and whose employees had discovered his drug abuse. The group had

\begin{footnotesize}
\textsuperscript{257} Id. 955-56.
\textsuperscript{258} Text accompanying note 273 et seq.
\textsuperscript{259} Text at note 256.
\textsuperscript{260} 738 N.W.2d 300, 306 (Minn. 2007).
\textsuperscript{263} 527 F.3d 412 (Gth Cir. La. 2008), cert. den 129 S. Ct. 631.
\end{footnotesize}
terminated the anesthesiologist for drug abuse but had not reported him to the state medical board or NPDB. Sixty-eight days after that termination members of the anesthesiology group submitted referral letters to a locum service that praised and recommended the physician yet failed to mention his drug abuse or that he had been terminated with a letter that included the phrase “[y]our impaired condition... puts our patients at significant risk.” The plaintiff medical center’s detailed credentialing request to the hospital where the anesthesiologist had previously been credentialed was replied to with a brief and neutral statement of the dates of his prior employment. At trial the jury found for the plaintiff medical center on claims of intentional and negligent misrepresentation, and awarded $8.24 million (the settlement and attorney’s fees in the original case).

On appeal the Fifth Circuit reversed the verdict against the hospital on the basis that under Louisiana law these facts did not give rise to an affirmative duty to disclose, a decision that may have been somewhat generous to the hospital and that may not be replicated in other jurisdictions. However, the court did affirm the judgment against the medical reference letter writers for affirmative misrepresentation, noting that “[t]hese letters are false on their face and materially misleading.”

Healthcare institutions making credentialing or hiring decisions currently face a dilemma when it comes to information about physicians contained in social network profiles. While there may be some risks in searching against them (as discussed in the next section), the potential liability for making a personnel decision in the absence of such information likely tips the balance.

B. Patients’ Health-Related Information Online

Health-related information posted online by patients might include open references to medical conditions or risk-taking (e.g., photographs of alcohol or drug abuse) or quite explicit signals of risky behaviors (e.g., membership of the Facebook page “I do stupid stuff when I’m Drunk”). Other signals may be more nuanced (e.g., membership of the Facebook fan page “A Glass of Wine Solves Everything”). Equally, membership in some social groups related to health conditions (although a relatively small number of persons join such groups) may operate as implicit signals regarding personal or

---

264 “The defendants did not have a fiduciary or contractual duty to disclose what it knew to [plaintiff]. And although the defendants might have had an ethical obligation to disclose their knowledge of (the anesthesiologist’s) drug problems, they were also rightly concerned about a possible defamation claim if they communicated negative information about [him].” 527 F.3d at 422.

265 527 F.3d at 419.


268 Social Life of Health Information, note 243, at 17. Only 6% of the cohort that looks for health information online “have started or joined a health-related group on a social networking site.”
family health (e.g., membership of Facebook group pages relating to Cancer Survivors, "Chronic Fatigue Syndrome," or Autism Awareness). Social network discussions by sufferers and survivors are frequently cited as an emergent area of powerful patient self-help. However, all such information may be of interest to employers or health insurers, and hopefully with more beneficence, physicians who search against their profiles.

I. Employers and Insurers

Published surveys in the general employment world suggest that somewhere from one-quarter to one-half of employers search the social network sites of potential employees. Surveyed employers took particular note of suggestions of alcohol or drug use, inappropriate photos or other posted information, and "unprofessional" screen names. Of course, sometimes, employee misconduct hardly needs any searching. The viral nature of data posted on social network sites is immense. For example, a video made by two pizza chain employees violating various health codes attracted one million views on YouTube (and felony charges for the employees).

Employer scrutiny of social network profiles implicates some legal risk when information discovered therein migrates into employment decisions. For example, under Federal law there is the potential for a discrimination action if a candidate was not hired because of, say, religious belief or a disability revealed or suggested on a social net-

269 http://www.facebook.com/group.php?gid=2214852731
270 http://www.facebook.com/group.php?gid=65675018622
272 See e.g., Zachary A. Goldfarb, Seeking a Cure, Patients Find a Dose of Conversation Online, WASH. POST, Jul. 21, 2008 at D01.
274 Adam Lisberg, Employers may be searching applicants' Facebook profiles, experts warn, DAILY NEWS, Mar. 10th 2008, http://www.nydailynews.com/money/2008/03/10/2008-03-10_employers_may_be_searching_applicants_fa.html (44% of employers searched profiles of job candidates on social networking sites, 39% searched a current employee's Facebook or MySpace page).
Some state laws prohibit a broader list of discriminations (e.g., sexual preference in California). Going further, some state laws apply privacy and non-discrimination principles to private activities by employees.\textsuperscript{278}

Information posted in the pseudo-secluded world of a social network site could signal certain genetic information.\textsuperscript{279} This issue is clearly on the radar of the Equal Employment Opportunity Commission (EEOC) as evidenced by a recent Notice of Proposed Rulemaking (NPRM) issued by the under the Genetic Information Nondiscrimination Act of 2008 (GINA).\textsuperscript{280}

GINA, signed into law in May 2008, broadly prohibits discrimination by employers and health insurers based upon genetic information. One of GINA’s key provisions is to characterize an “employer,” “employment agency,” “labor organization” or “labor-management committee controlling apprenticeship or other training or retraining” that “request[s], require[s], or purchase[s] genetic information with respect to an employee or a family member of the employee…” as having engaged in an “unlawful employment practice.” GINA offers several safe harbors including:

where an employer purchases documents that are commercially and publicly available (including newspapers, magazines, periodicals, and books, but not including medical databases or court records) that include family medical history.\textsuperscript{281}

In the EEOC’s 2009 NPRM under GINA this exception is expanded to include “electronic media, such as information communicated through television, movies, or the Internet, except that a covered entity may not research medical databases or court records, even where such databases may be publicly and commercially available, for the purpose of obtaining genetic information about an individual.”\textsuperscript{282} In its commentary.

\textsuperscript{278} Civil Rights Act of 1964 (Title VII), Americans with Disabilities Act of 1990 (Titles I & V).
\textsuperscript{279} See e.g., Colo. Rev. Stat. § 24-34-402.5(1) (“It shall be a discriminatory or unfair employment practice for an employer to terminate the employment of any employee due to that employee’s engaging in any lawful activity off the premises of the employer during nonworking hours…”). See also Cal. Lab. Code, § 96(k).
\textsuperscript{280} For example, signals about family concerns regarding Type I/ /Juvenile diabetes. See Facebook Fan Page (Find a Cure for Juvenile Diabetes). http://www.facebook.com/s.php?q=diabetes&n=-1Bk=40000000000106s=f=6init=q6sid=f7071Hayaa1956a04717D1f9888657f#group.php?gid=22048l909. See also Facebook Fan Page (Sickle Cell Anemia Disease).
EEOC invited “public comment on whether there are sources similar in kind to those identified in the statute that may contain family medical history and should be included either in the group of excepted sources or the group of prohibited sources, such as personal Web sites, or social networking sites.” An EEOC decision to take the latter approach and to wall-off genetically-related social network data from employer or insurer use would signal the first use of an inalienability rule in the social network regulatory space.

In the meantime employers and insurers likely will argue that the law of boundaries has little relevance to their activities. First, the Intrusion tort would not apply to a non-corporeal (or informational) seclusion. Second, any Publicity action should fail because the information searched is not “private” as it has been disclosed to the social network user’s “friends,” while the use of the discovered information does not satisfy the “publicity” requirement: the broadcast “public” channel property is inapplicable and because the information is only used “internally,” plaintiff cannot meet the numerical touchstone required for “private” channel cases.

The decisional law suggests some validity regarding the second of these Publicity arguments, at least in most cases of minimal distribution. Notwithstanding and as argued below, the information should be viewed as “private” when the user has applied privacy and security settings.

However, employers and insurers should be less sanguine about the inapplicability of the Seclusion tort. Case law already recognizes areas of seclusion in otherwise public areas; the question that is open is whether an application of security and privacy settings will be the touchstone for delineating a secluded space. The non-corporeal argument is more difficult. To an extent the courts will face a core entitlement question: whether to consign to history the trespass-like roots of the Intrusion tort and apply it more liberally to informational privacy. If they take this latter, less existential, approach the appropriate doctrinal solution will be to pivot the tort around the offensiveness of the intrusion rather than the locus of the seclusion.

2. Physician Use of Posted Social Information

Employers and health insurers may have understandable business reasons for searching online profiles. But, should physicians research their patients? And what should be done with such information diagnostically?

Of course, not all patient-posted information allows for identification of specific patients. As such, aggregated discussions by de-identified patients provides an educational opportunity for physicians who wish to learn more about generalized care models.

---

288 Id. at page 9063.
288 See discussion at note 100.
290 See discussion at note 98.
and patient perceptions and experiences associated with particular illnesses or diseases.\textsuperscript{291}

However, Moreno and colleagues examined the profile pages of self-described 16 and 17 year-olds in the “class of 2008” MySpace group, and found that most were identifiable by name, photograph, location and that “[n]early half of the adolescents . . . publicly disclosed sexual activity, alcohol use, tobacco use, or drug use.”\textsuperscript{292} A similar study of 16-18 year-olds across several social network sites by Williams and colleagues found “84\% of profiles and blog discussions containing some type of risk-taking behaviors,” with nearly 50\% of the participants at some risk of specific identification.\textsuperscript{293}

The availability of this type of patient-specific information creates a classic “emerging technology” problem for physicians. Ethically and legally may they access such information and, if they do, will they create a standard of care requiring scrutiny of such online data? The first question is easier to answer; general ethical standards suggest that physicians ask their patients’ permission to access such information, even if it is publicly available. This stance dovetails with good risk management in that obtaining not just consent but informed consent regarding the access and use of such data will reduce the likelihood of either intrusion or malpractice actions. The second question, going to the standard of care, is harder. At the very least professional specialty organizations (e.g., the American Psychiatric Association) should consider developing clinical practice guidelines on the subject with a view to preempting the indeterminacy of case-by-case development of the standard of care.

3. Third Parties Posting Patient Information

Physicians will seldom be the direct source for patient-related health information that finds its way onto a social network site. Patients themselves, or their “friends” will have posted most such data. Some information may be sourced from providers (itself potentially implicating breach of confidence or HIPAA) but posted by meddlesome third parties.\textsuperscript{294} Here, publicity and breach of confidence actions still may be applicable. The controversies in the recent Minnesota case of \textit{Yath v. Fairview Clinics},\textsuperscript{295} began with a patient visit to a hospital clinic for STD testing. An acquaintance related to the patient’s


\textsuperscript{292} Megan A. Moreno, MD, MSEd; Malcolm Parks, PhD; Laura P. Richardson, MD, MPH, \textit{What Are Adolescents Showing the World About Their Health Risk Behaviors on MySpace?} \textit{MEDGENMED}, 2007; 9(4): 9.

\textsuperscript{293} Williams AL, Merten MJ., \textit{A review of online social networking profiles by adolescents: implications for future research and intervention} \textit{ADOLESCENCE}. 2008 Summer;43(170):253-74.

\textsuperscript{294} See e.g., Meade v. Orthopedic Assocs. of Windham County, 2007 Conn. Super. LEXIS 3424 (Conn. Super. Ct. Dec. 27, 2007) (employee acquired and distributed patient records but action only filed against health facility; held, “(a) cause of action for invasion of privacy will not lie where the defendant did not directly publicize the private facts about the plaintiff even though ‘publicity was a natural and foreseeable consequence’ of the defendant’s actions”). Of course the institution may be responsible vicariously in some circumstances and might still face HIPAA liability.

\textsuperscript{295} 2009 Minn. App. LEXIS H7 (2009).
husband worked at the clinic as a medical assistant. She recognized the patient and subsequently accessed her electronic medical record. There she discovered the patient’s positive STD test and the fact that the patient had a new sexual partner. The medical assistant passed on the information to another employee and the information eventually became known to the patient’s estranged husband. After an investigation the medical assistant was terminated by the hospital. Shortly thereafter a MySpace page was created containing information from the patient’s medical record. The page was online for approximately 24 hours and likely was viewed by only six people. The patient brought action against most of the actors and the hospital on several theories including public disclosure of private facts and the private right of action provided by Minnesota’s Health Records Act. The trial court granted the defendants’ motions for summary judgment.

On appeal the court remanded the issue of the statutory private right of action asserted by the patient against the Hospital and the medical assistant to the trial court, but not before ruling that such a state private right of action was not preempted by the federal HIPAA code, ruling that the provisions were complementary: “[r]ather than creating an ‘obstacle’ to HIPAA, [the state law] supports at least one of HIPAA’s goals by establishing another disincentive to wrongfully disclose a patient’s health care record.” A similar analysis should apply to a common law action for breach of confidence by a healthcare provider.

The Yath court affirmed the summary judgment on the public disclosure count on the basis that the likely authors of the MySpace page had been dismissed from the action. Notwithstanding, the court exhaustively examined the defendant’s other contention that the “publicity” requirement (discussed above) was not satisfied by posting to a social network site that was only available for a short time and viewed by a small number of people. The court referenced a controlling Minnesota analysis of Restatement (Second) section 652D establishing the “publicity” element was satisfied by proving either: “a single communication to the public.” or “communication to individuals in such a large number that the information is deemed to have been communicated to the public.”

\[296\] Id. at *4
\[297\] Id.
\[298\] Id. at *5.
\[299\] Id.
\[300\] Id. at *7.
\[301\] Id.
\[302\] Id.
\[303\] Minn. Stat. § 144.335 governed the case but has been replaced by Minn. Stat. § 144.298.
\[305\] Id. at 38.
\[306\] Text accompanying note 169.
\[307\] Bodah v. Lakeville Motor Express, Inc., 663 N.W.2d 550, 553 (Minn. 2003).
\[308\] 2009 Minn. App. LEXIS at *16.
The court viewed posting to a social network site as an example of the former type of public communication because “[t]his Internet communication is materially similar in nature to a newspaper publication or a radio broadcast because upon release it is available to the public at large.”

Analogizing this brief web posting to “a late-night radio broadcast aired for a few seconds and potentially heard by a few hundred (or by no one)” or “a poster displayed in a shop window,” the court noted:

It is true that mass communication is no longer limited to a tiny handful of commercial purveyors and that we live with much greater access to information than the era in which the tort of invasion of privacy developed. A town crier could reach dozens, a handbill hundreds, a newspaper or radio station tens of thousands, a television station millions, and now a publicly accessible webpage can present the story of someone’s private life, in this case complete with a photograph and other identifying features, to more than one billion Internet surfers worldwide. This extraordinary advancement in communication argues for, not against, a holding that the MySpace posting constitutes publicity.

The Yath court specifically noted that the MySpace profile in question was not one to which access had been restricted by “a password or some other restrictive safeguard.” Thus, it left hanging the same question as the court in Morena v. Hanford Sentinel, Inc., where, as previously discussed, a college student’s MySpace posting, critical of her hometown, found its way to the local newspaper. If a social network site user applies security and privacy settings would that render the site “secluded” for the purpose of initiating a breach of seclusion action or “private” for the purpose of resisting a publicity claim?

The most efficient approach for courts to adopt would be a bright line “posting” rule; that is, all posts, security or privacy settings notwithstanding, are public. Such an approach would avoid the inevitable and possibly interminable case-by-case debates as to whether “private” exposure of information to 10, 100, or even 1000 friends would be akin to a public post.

However, that approach seems contrary to Hill v. National Collegiate Athletic Assn., otherwise followed in Morena. Hill upheld the NCAA’s drug testing program in a suit brought by student athletes arguing violation of California’s constitutional right to privacy. Subsequently, it may be have been narrowed by the Supreme Court of California in...
Sheehan v. San Francisco 49ers, Ltd.\textsuperscript{316} a case dealing with security pat-downs at a football stadium. Sheehan re-emphasized Hill’s statement about context; that “assessment of the relative strength and importance of privacy norms and countervailing interests may differ in cases of private, as opposed to government, action.”\textsuperscript{317} Sheehan also stressed the Hill observation that a plaintiff’s privacy interests when bringing an action under California’s constitutional privacy right “may weigh less in the balance”\textsuperscript{318} if he or she “was able to choose freely among competing public or private entities in obtaining access to some opportunity, commodity, or service.”

Yet, in the context of the common law of boundaries, Hill’s words remain potent.

Privacy rights … have psychological foundations emanating from personal needs to establish and maintain identity and self-esteem by controlling self-disclosure: “In a society in which multiple, often conflicting role performances are demanded of each individual, the original etymological meaning of the word ‘person’—mask—has taken on new meaning. [People] fear exposure not only to those closest to them; much of the outrage underlying the asserted right to privacy is a reaction to exposure to persons known only through business or other secondary relationships. The claim is not so much one of total secrecy as it is of the right to define one’s circle of intimacy—to choose who shall see beneath the quotidian mask. Loss of control over which ‘face’ one puts on may result in literal loss of self-identity [citations], and is humiliating beneath the gaze of those whose curiosity treats a human being as an object.”\textsuperscript{320}

The key privacy expectation acknowledged by the law of boundaries is this “right to define one’s circle of intimacy.” As citizens spend more of their time in online environments and make responsible use of privacy and security settings to disaggregate those with whom they interact, so the law should respect their defined circles of intimacy.

C. Physicians and Patients as “Friends”

Suppose a physician “friends” a patient or vice versa. Does such blurring of personal and professional relationships create concern in either the legal or ethical domains? In the case of the former the primary question will be whether such a blurred, technologically mediated relationship could give rise to the legally significant physician-patient relationship.\textsuperscript{321} In the ethical domain the question will come down to motive: is there a

\textsuperscript{316} 45 Cal. 4\textsuperscript{th} 992 (2009).
\textsuperscript{317} 7 Cal. 4\textsuperscript{th} at 38 cited at 45 Cal. 4\textsuperscript{th} at 1001.
\textsuperscript{318} Hill, 7 Cal.4th at 39, quoted in Sheehan, 45 Cal. 4\textsuperscript{th} at 1002.
\textsuperscript{319} Id.
\textsuperscript{320} 7 Cal. 4\textsuperscript{th} at 25, quoting Briscoe v. Reader’s Digest Association, Inc. 4 Cal.3d 529 (1971).
\textsuperscript{321} A related question is whether physician-patient contact through a social network could constitute the continuation of a relationship for the purposes of tolling a period of limitation. See e.g., Griffith v Brant.
sense that the relationship is driven by the needs of the physician rather than the interests of the patient?

Again, context is important in unpacking the boundary issues. The appropriate question must be whether social or professional interests motivate the physician who follows a patient on Facebook or Twitter. If the motivation is social then difficult boundary issues may arise. If professional (e.g., using social media to extend the treatment space), difficult risk management questions arise.

1. Creating a Physician-Patient Relationship

Most of the scenarios discussed in this article assume the existence of a physician-patient relationship and then discuss how physician or patient online activities will play out against the healthcare regulatory matrix. Discussed, therefore, are scenarios such as physicians searching their patients’ social network sites or micro-blogging about their treatment. Suppose, however, that there is no formed professional relationship at the point when a patient and a physician interact online. Could such interaction trigger the creation of a “physician-patient relationship”?

Such a relationship is both a conclusion and a term of art relied upon by the ethical and legal domains. As an ethical construct, it is the foundation of duties (and correlate expectations) of competence, respect, and confidence. In the legal domain, the existence of a “physician-patient relationship” establishes the contractual responsibilities of the parties (such as the provision of services and the obligation to pay) and is the predicate for the finding of a legal duty; a requirement for tort recovery in the case of negligently provided care.

These domain-specific questions engender the question—what does it take to create the physician-patient relationship? The doctrinal answer is that “the relationship is created when professional services are rendered and accepted for purposes of medical treatment.” The existence of a physician-patient relationship frequently is stated to be a jury issue. In practice, therefore, the key issue is where the courts draw the summary judgment line.

Because of the consensual nature of the physician-patient relationship the rabbit
chased by the courts in these cases is whether the physician consented to treat the patient.\textsuperscript{326} Such consent can be express, implied,\textsuperscript{327} or derived from a duty owed by the physician to another;\textsuperscript{328} in short, “whatever circumstances evince the physician’s consent to act for the patient’s medical benefit.”\textsuperscript{329} This approach explains most of the decisions related to the clusters of fact-patterns that are relatively mature; for example, how courts navigate the distinction between the informal (or “curbside”) consult\textsuperscript{330} and the formal (or “bedside”) consult,\textsuperscript{331} deal with the responsibilities of on-call but non-treating physicians,\textsuperscript{332} and respond to cases where patients are examined by physicians employed by others such as employers or insurers.\textsuperscript{333}

The cases dealing with technologically mediated, but not physical contact between physician and patient are less transparent. It does seem clear that “a telephone call merely to schedule an appointment with a provider of medical services does not by itself establish a physician-patient relationship where the caller has no ongoing physician-patient relationship with the provider and does not seek or obtain medical advice during the conversation.”\textsuperscript{334} Similarly, merely scheduling a diagnostic test is likely insufficient.\textsuperscript{335} However, as soon as there is engagement in the treatment process by the physician, the relationship may be held to exist.\textsuperscript{336}

The case that is closest to a social network scenario is \textit{Miller v. Sullivan}, where a dentist telephoned a friend, a physician (but not his physician) between 9:30-10:00 a.m., and informed him that he believed he was having a heart attack. The physician allegedly told the dentist “to come over and see him right away.”\textsuperscript{337} However, the dentist continued to see his own patients through the morning and did not reach the physician’s

\textsuperscript{326} “The physician may consent to the relationship by explicitly contracting with the patient, treating hospital, or treating physician. Or the physician may take certain actions that indicate knowing consent, such as examining, diagnosing, treating, or prescribing treatment for the patient.” Lownsbury v. VanBuren, 762 N.E.2d 354, 362 (Ohio 2002).
\textsuperscript{327} See e.g., St. John v. Pope, 901 S.W.2d 420, 424 (Tex. 1995).
\textsuperscript{329} Lownsbury v. VanBuren, 762 N.E.2d 354, 390 (Ohio 2002).
\textsuperscript{331} See e.g., Kelley v. Middle Tenn. Emergency Physicians, P.C., 133 S.W.3d 587 (Tenn. 2004).
\textsuperscript{332} See e.g., Wazevich v. Tasse, 2007 Ohio App. LEXIS 4484 (Ohio Ct. App., Cuyahoga County Sept. 27, 2007); Prosise v. Foster, 344 S.E.2d 331 (2000).
\textsuperscript{335} Jackson v. Isaac, 76 S.W.3d 177, 184 (Tex. App. 2002).
office until the early afternoon at which point he suffered a cardiac arrest.\textsuperscript{338} The court upheld the defendant physician’s summary judgment.\textsuperscript{339} Unfortunately, it did so on more than one ground (no duty of care and no breach) stating.

Assuming that a physician renders professional service for purposes of medical treatment to a prospective patient who calls on the telephone when the physician tells the caller to come to his office right away, the record in this case conclusively establishes that decedent did not accept the professional service. Instead, decedent chose to pursue an entirely different course of conduct than that recommended by defendant.\textsuperscript{340}

In conflating the issues of duty and breach, the \textit{Miller} court made it less than clear whether a physician-patient relationship existed on these facts. However, arguably the court held that there was no such relationship because (and this is a different approach from the cases discussed above) the patient failed to agree to the relationship by rejecting the physician’s advice.

Physicians seem to understand the perils of creating an unexpected, offline physician-patient relationship. They show caution in social interactions (e.g., at social gatherings, parties, etc.). This caution will need to be extended to online interactions.

In the absence of a pre-existing physician-patient relationship the blog scenario gives rises to issues that are similar to those encountered by physicians in navigating email questions about health; more specifically, responding to unsolicited email.\textsuperscript{341} When a non-patient poses a health-related question to a physician, be it through an email, a blog, or a social network site, the physician has two core options: to ignore the question or to answer it. Ignoring such a communication is not without some risks, particularly if the putative patient describes an emergency situation.\textsuperscript{342} However, any kind of personalized response, let alone any type of diagnosis or treatment advice would likely create a jury issue over the creation of a physician-patient relationship, even if disclaimers accompanied the communication.\textsuperscript{343} Rather, the only legally sound approach is for the physician to respond to an electronic inquiry with a standard form response (that in no way refers to the specific sender or the sender’s disclosed information) that (1) informs the questioner that the physician does not answer such online questions, (2) supplies the questioner with the physician’s offline office information in case the questioner

\begin{verbatim}
\textsuperscript{338} Id. at 823
\textsuperscript{339} Id. at 824.
\textsuperscript{340} 214 A.D.2d at 823.
\textsuperscript{341} See generally Gunther Eysenbach, MD; Thomas L. Diepen, MD, PhD, Responses to Unsolicited Patient E-mail Requests for Medical Advice on the World Wide Web, JAMA. 1998;280:1333-1335.
\textsuperscript{342} Cf. Patricia C Kuszler, MD, JD, A Question of Duty: Common Law Legal Issues Resulting from Physician Response to Unsolicited Patient Email Inquiries, J MED INTERN RES. 2000 Jul–Sep; 2(3): e17; MV Seeman & B Seeman, E-psychiatry: The Patient-Psychiatrist Relationship in the Electronic Age,161 CANADIAN MED. ASS’N J, 1147 (1999) (“Clearly, the most judicious course of action is not to respond to email queries.”).
\textsuperscript{343} Cf. Eric E Shore, Giving advice on social networking sites, Vol. 85, No. 5, pg. 18, MEDICAL ECONOMICS, Mar 7, 2008.
\end{verbatim}
would like to make an appointment, and (3) provides contact information for the emergency services and suggest the questioner contacts same if he or she cannot wait for an appointment during regular business hours.

2. Risk-Managing a Blurred Relationship

The correlate of this scenario also requires attention. If one assumes an existing physician-patient relationship and that the physician is utilizing social network tools to extend the treatment space, what are the liability risks? Regarding the use of email communication between patient and physician the AMA stresses notification by the physician to the patient of the risks and limitations of such communication. These include, “potential breaches of privacy and confidentiality, difficulties in validating the identity of the parties, and delays in responses.” Any such communication should be preceded by informed consent regarding these risks. Absent such setting of professional and technological expectations (and boundaries) liability risks may arise if a physician is not checking social network posts regularly (or regularly as the patient posts) and fails to see, say, a time-sensitive diagnostic signal.

3. Appropriateness of “Friend” Relationships

Suppose that there is an extant physician-patient and, hence professional relationship, but that a social or personal relationship subsequently develops through a social network intermediary. This phenomenon has received the most commentary regarding employment relationships. E.g., when employers seek to “friend” employees and/or exploit access to posted data such as opinions or photographs.

At the extreme, social relationships between physicians and patients can involve sexual relationships. The AMA characterizes “[s]exual contact that occurs concurrent with the patient-physician relationship” as “sexual misconduct.” Non-concurrent relationships may also be unethical “if the physician uses or exploits trust, knowledge, emotions, or influence derived from the previous professional relationship.”

---

345 Id. at Opinion 5.026(4).
349 AMA, CODE OF MEDICAL ETHICS § B.14 - Sexual Misconduct in the Practice of Medicine.
350 Id.
concepts of trust, exploitation, and the primacy of patient well-being help to tease out the application of ethical principles to “friending” online. Nadelson and Notman have helpfully explored these greyer areas of physician-patient relationships. They differentiate between “minor boundary crossings” that they do not regard as “exploitative” from those that they categorize as “damaging boundary violations.” For the purposes of this article, the vocabulary Nadelson and Notman use to frame the issues is on point here. In particular, they state:

An essential element of the physician’s role is the idea that what is best for the patient must be the physician’s first priority. Physicians must set aside their own needs in the service of addressing their patient’s needs. Relationships, such as business involvements, that coexist simultaneously with the doctor–patient relationship have the potential to undermine the physician’s ability to focus primarily on the patients’ well being, and can affect the physician’s judgment.

Some physicians argue that the use of social network tools to extend the physician-patient relationship allows the patient to see the “human side” of the physician. However, as Nadelson and Notman observe, “at times self-disclosure may be excessive and create difficulties. The patient may react negatively and it may seem like a role reversal if the doctor begins to disclose personal problems to the patient,” and can create a “boundary problem because it can use the patient to satisfy the doctor’s own needs for comfort or sympathy.” Specific ethical guidelines consistent with this approach caution physicians regarding, for example, discussion of politics or “derogatory language or actions.” In short, the physician must be protective of the patient’s needs, and not his own.

---

352 Id. at 195. See also APA, THE PRINCIPLES OF MEDICAL ETHICS WITH Annotations ESPECIALLY APPLICABLE TO PSYCHIATRY, 2009, Section I, Annotation I. http://www.psych.org/MainMenu/PsychiatricPractice/Ethics/ResourcesStandards.aspx (“A psychiatrist shall not gratify his or her own needs by exploiting the patient”).
354 Id. at 197.
D. Physicians “Tweeting” or Posting About Their Work

The modern Hippocratic oath will include language such as “I will respect the hard-won scientific gains of those physicians in whose steps I walk, and gladly share such knowledge as is mine with those who are to follow.” The AMA Code of Medical Ethics includes in its description of the physician’s role, “a teacher who imparts knowledge of skills and techniques to colleagues.” Not surprisingly physicians embrace new technologies to fulfill their educational responsibilities. However, posting or “tweeting” about their work is not without its risks.

1. Blogging and Posting

According to 2008 research, 12 percent of Internet users (9 percent of all U.S. adults) “blog,” while 33 percent of Internet users (24 percent of all adults) read blogs. Kovic and colleagues estimated that there are over one thousand active English-language medical blogs, and found that these medical bloggers are highly educated and that many had previously published scientific papers. However, only a relatively small number of participants in the medical blogosphere identified themselves as healthcare professionals. Seeman identified the six most highly used health-related blogs as BadScience.net (written by a U.K. physician who critiques media coverage of science), Medgadget.com (written by MDs and biomedical engineers), the journalist-run Wall Street Journal Health Blog, SharpBrains (concentrating on “brain fitness” and “the cognitive health market”), KevinMD.com (written by a New Hampshire-based primary care physician; its associated Twitter site, @kevinmd, has more than 9,000 “followers”), and Diabetes Mine (a patient information and support blog).

Lagu and colleagues examined 271 blogs written by healthcare providers. 42.1 percent described interactions with individual patients. 16.6 percent included information that

---

362 http://badscience.net/.
365 http://www.sharpbrains.com/blog/.
366 http://www.kevinmd.com/blog/.
could identify the provider or themselves, while eight blogs included imaging related to patients and three blogs even showed identifiable photographs. Patients were portrayed negatively in 17.7 percent of blogs; negative comments about the healthcare system appeared in 31.7 percent of blogs.368

Certain types of blog posts, with different levels of attendant risk, can be identified.369 The first, which will pose few legal risks, may be thought of as “peer blogging,” where healthcare providers seek to reach out to their colleagues much like they do in offline channels such as medical journals or even professional conferences, discussing new treatments, drugs, or technologies.

The second is the “ranting” blog post, where physicians might vent about salaries, low health care reimbursement rates, long working hours and other issues that frustrate them.370 Such posts could generate unwelcome attention from peers, institutional providers, or medical boards. Suppose, for example, that a physician posted, “I had an case today dealing with a patient previously seen by Dr. Smith; I spent the best part of the day putting right what he did wrong!” Such a communication is likely to get the attention of the peer who could sue for defamation.371 It might also attract scrutiny from professional organizations or medical boards for unethical conduct,372 and could violate the terms of a contract with an employing or credentialing healthcare institution.

The highest level of risk is associated with a blog posting that involves the risk of a

369 See generally Web risk: Blogging can be a medically useful tool for doctors; but details could doom your career. MISSOURI MEDICAL LAW REPORT, June 2008 (interview with Nicolas Terry); Deirdre Kennedy, Doctor Blogs Raise Concerns About Patient Privacy, NPR, June 1, 2009, http://www.npr.org/templates/story/story.php?storyId=88163567.
370 See Scott R. Grubman Note, Think Twice Before You Type: Blogging Your Way To Unemployment, 42 GA. L. REV. 615 (2008). See also, David Kravets, AP Reporter Reprimanded For Facebook Post; Union Protests, WIRED, June 9, 2009 (discussing various adverse employment disciplinary actions brought by employers against Facebook-posting employees).
371 “In a suit for defamation, a private plaintiff must allege (1) publication of false statements about the plaintiff that ‘expose [] [him] to distrust, hatred, contempt, ridicule or obloquy or which cause [] to be avoided, or which [have] a tendency to injure [] in his office, occupation, business or employment,’ Saud v. Maroun 2009 U.S. Dist. LEXIS 42574, *10 (M.D. Fla. May 20, 2009) (citing Cooper v. Miami Herald, 129 Fla. 236, 31 So. 2d 382, 384 (Fla. 1947)); (2) done without reasonable care as to the truth or falsity of those statements; and (3) that result in damage to that person.” Id (citing Hoy v. Independent Newspapers, Inc. 450 So. 2d 293, 294–95 (Fla. 2d DCA 1984)). In Saud, the court found that the defendant’s allegations published on a blog that the plaintiff was an unemployed lawyer and that his car was purchased with stolen money to be triable as to whether they satisfy elements these three elements of a defamation suit. Id at II–II. The court further found that even though the blog was political in tone, there was a sufficient mix of fact and opinion to be reasonably construed as defamation. Id at 14. In the example cited, the fact that the discussion would likely be predicated on an actual patient or health problem would make it easier for courts find defamatory statements when mixed with opinion. Id. Also that First Amendment protection for derogatory blog posts will be limited. See e.g., Richerson v. Beckon, 2009 U.S. App. LEXIS 12870 (5th Cir. Wash. June 16, 2009) (Defense summary judgment upheld in § 1983 action by teacher against supervisor who was transferred after making comments on her personal blog).
372 See, for example, AMA Opinion 9.031 - Reporting Impaired, Incompetent, or Unethical Colleagues, http://www.ama-assn.org/ama/pub/physician-resources/medical-ethics/code-medical-ethics/opinion9031.shtml, that specifies how such issues should be dealt with.
patient being identified. Here, both the breach of confidence tort and HIPAA may be implicated. Physicians may use pseudo anonymous terms to describe the cases they reference in an attempt to reduce the possibility of positively identifying any patient in a blog discussion. Notwithstanding such efforts, re-identification may be possible from detailed demographics, location, as well as symptoms. Discussing general breaches of confidentiality, Brann & Mattson note, “[u]nintentional confidentiality breaches have been overheard in elevators, cafeterias, hallways, doctors’ offices, and hospital rooms and at cocktail parties.”373 The authors’ typology of breaches included disclosures by healthcare providers to their own family members374 and to their friends.375 As they describe in the latter context (which is analogous to social network posts), “[i]n providing confidential information to friends, healthcare providers run an even greater risk of harming patients. This is because they may not be as aware of their friends’ extended network of relationships as they are of their family’s. Consequently, they may have even less control over who else might become privy to the confidential information.”376

2. Twitter Feeds and Status Updates

In February 2009, a surgeon at Henry Ford Hospital in Detroit provided a real-time Twitter feed during his performance of a robotic partial nephrectomy on a 60 year-old patient.377 This was not a rogue surgeon indulging a personal interest. Dr. Craig Rogers is a well-known urologist and the feed, written by his chief resident, was publicized in advance by his hospital system.378 The avowed purpose of the feed was “to get the word out” about less invasive surgical techniques.

As previously noted, the AMA Code of Ethics mandates that either contemporaneous or recorded observations of physician-patient interactions must be preceded by explicit agreement and comprehensive informed consent. Separate consents are required both for the original recording and any subsequent broadcast. The consent must state that patient’s decision will not affect the medical care he or she receives.380

These general rules are reinforced by various ethics opinions from specialty organizations.381 For example, in answer to the question, “May I use a videotape segment of a

---

374 Id. at 244-45.
375 Id. at 245.
376 Id. at 245.
380 Text at note 212.
381 See e.g., APA, THE OPINIONS OF THE ETHICS COMMITTEE ON THE PRINCIPLES OF MEDICAL ETHICS, at 24 (Informed con-
therapy session at a work-shop for professionals?” the American Psychiatric Association listed the following preconditions:

1. The patient gives fully informed, uncoerced consent that is not obtained by an exploitation related to the treatment.

2. The proposed uses and potential audience are known to the patient.

3. No identifying information about the patient or others mentioned will be included.

4. The audience is advised of the editing that makes this less than a complete portrayal of the therapeutic encounter.\(^{382}\)

The common law privacy rules are consistent. Recall \textit{Vassiliades v. Garfinckel’s}, where a physician published before and after photographs of his patient via a television commercial.\(^{383}\) The court found “the nature of the publicity ensured that it would reach the public.”\(^{384}\) It seems reasonably clear that public Twitter feeds or unsecured Facebook pages will satisfy the courts’ emerging approach to “public” disclosure as discussed in \textit{Yath}.\(^{385}\) As evidenced by the increased use of such feeds by public entities (such as police departments), this is a broadcast medium designed to reach the public.\(^{386}\)

The specific difficulty faced by physicians using social network real-time broadcast technologies such as Twitter feeds or Facebook status updates is how to satisfy the ethical and legal requirements of consent. Informed consent does not scale well and application of consent requirements analogous to filming or broadcasting patient treatments include quite specific (and close to impossible) requirements of the disclosure of the audience that will see the broadcast. Arguments that the patient was anonymous (or, in HIPAA terms, that the patient information was de-identified) may not be sustainable given the likelihood that some in a public audience would be able to deduce the identity of the patient (there are only so many persons of a certain age being treated for a particular ailment in an identifiable hospital or locale).


\(^{385}\) Text accompanying note 295

One blogger has published “140 Health Care Uses for Twitter” and, perhaps, physicians pushing status updates from an E.R. honestly believe that they are educating others about the practice of medicine. However, if either the tweeting or the blogging is about patients, the admonition from Nadelson and Notman requires reiteration: “what is best for the patient must be the physician’s first priority.”

V. Conclusion

The issues examined in this article are about context. For many readers there may be no issue deserving of legal resolution—merely bemusement that anyone would act online in a manner analogous to wearing a t-shirt proclaiming “I Like Weed” or “If you can Read this, I’ve been Paroled” to a job interview. Similarly, it may be argued that the legal system should not rescue those with bad judgment or concern itself with risky behavior that is exposed to all by users who fail to make appropriate use of available privacy or security settings. As more people lose their jobs or their health insurance because of what they post online perhaps more users will employ these settings to disaggregate their “friends” or otherwise modulate their online behavior. Equally, healthcare institutions, teaching hospitals, and physician organizations are likely to make their views about the online behavior of their physicians far more pointed and embed them in normative form. From there such norms are likely to migrate to our legal and regulatory systems.

The “soft” (even soft law) answers to many of the issues discussed in this article are, first, to increasingly incorporate the issues raised into professional training and institutional risk management strategies. Second, observe as press and public opinion (combined with “nudges” from regulatory agencies such as the FTC) force social network sites to increase the number and transparency of protective online tools they make available to users. However, changes to their architectures, such that robust privacy and security settings become the default, challenge aspects of the services’ business models and likely will not occur soon, or willingly. Third, whatever the EEOC ends up proposing with regard to social network data and GINA, we are likely to see legislatures or regulatory agencies fashion some bright lines as to when posted data can or cannot be used in some contexts or by some persons.

However, beyond (and, perhaps, before) such amelioratory strategies, the common law of boundaries must step up and protect responsible users online. True to its context-based framework the law of boundaries should recognize private or secluded areas that have been established by users of social network sites.

388 Text accompanying note 351.