Social Media Law & Policy Report™

February 10, 2015

Health

Patient Privacy in the Digital Age and Disclosure on Social Media

HEALTH

Privacy concerns—in particular regarding sensitive information about patient health on social media—are likely to increase over time, the authors write. The tradeoff, though, may be significant benefits to patients in the long run. They address the benefits and risks of patients sharing their health information in the digital age.

By Sharon E. Roberg-Perez and Kristine A. Tietz

Sharon Roberg-Perez is a principal at Robins Kaplan LLP in the firm's Intellectual Property and Technology Litigation group. She is an MIT-trained Ph.D., with a practice focused on biotechnology, medical devices and digital health.

Kristine Tietz is an associate at Robins Kaplan LLP in the firm's Intellectual Property and Technology Litigation group. Kristine represents clients in patent, copyright and trademark disputes across a diverse spectrum of industries.

Big Brother has nothing on Mark Zuckerberg. Who needs surveillance cameras when over 1.3 billion people willingly disclose who they are, where they live, what they do for a living and the names (and preferences) of their children, closest friends and pets? [1] Going forward, we can expect even more digital disclosure of personal information, some of it quite sensitive. Facebook and other high-tech giants, most notably Google and Apple, are looking to the health-care field to drive growth. [2] T he social media giant is reportedly developing health and wellness apps, as well as building virtual, patient support communities. [3]

[1] Statistic Brain, Facebook Statistics, http://www.statisticbrain.com/facebook-statistics.

[2] Christina Farr & Alexei Oreskovic, Exclusive: Facebook Plots First Steps Into Healthcare, Reuters, Oct. 3, 2014, available athttp://www.reuters.com/article/2014/10/03/us-facebook-health-idUSKCN0HS09720141003.

[3] Jof Enriquez, As Facebook Turns Toward Healthcare, Social Media Privacy Concerns Increase, Nuviun, Oct. 21, 2014, available athttp://nuviun.com/content/news/as-facebook-turns-toward-healthcare-social-media-privacy-concerns-increase-.

Are patients likely to adopt digital health-care initiatives by the Internet behemoths? And, if so, why? It is hardly a secret that Google can track each query that is made using its search engine or browser, leave identifying cookies on your computer, and cross-reference your IP address to get a pretty good idea of your name, address and phone number. [4] Moreover, social media sites such as Google+, YouTube and Facebook have access to a wealth of information about their users and a good deal of latitude regarding how they can use that information. An individual's collective cyberspace history may be “far more intimate” than expected, revealing a “detailed portrait of [her] life and interests.” [5] In light of this, what do patients possibly stand to gain by sharing their health information in cyberspace?

[4] Caitlin Dewey, Everything Google Knows About You (and How It Knows It), Washington Post, Nov. 19, 2014, available athttp://www.washingtonpost.com/news/the-intersect/wp/2014/11/19/everything-google-knows-about-you-and-how-it-knows-it/; Robert Epstein, Google's Gotcha: 15 Ways Google Monitors You, U.S. News & World Rep., available athttp://www.usnews.com/opinion/articles/2013/05/10/15-ways-google-monitors-you.

[5] Dewey, supra note 4.

Benefits of Participation

For starters, patients gain a sense of community. Online health communities offer an abundance of information for patients

and their caregivers, family and friends. More than half of the members of PatientsLikeMe, an online patient community established over a decade ago, report that the site was either moderately or very helpful for learning about their symptoms. Over half said that the site helped them manage their symptoms and better understand treatment options. And nearly half said that it was the connection with another member that was critical to being able to learn about options. [6] In and of itself, a feeling of "belonging" can improve quality of life by positively impacting physical and mental health. [7]

[6] Paul Wicks et al., Sharing Health Data for Better Outcomes on PatientsLikeMe, 12 J Med. Internet Res. No. 2 (2010).

[7] See e.g. Karen Windle et al., Preventing Loneliness and Social Isolation: Interventions and Outcomes, Social Care Institute for Excellence, at 3, available athttp://www.scie.org.uk/publications/briefings/briefing39/ (registration required).

What is perhaps even more significant is the relationship between the digital sphere and a growing sense of patient autonomy. Within the past two years, 72 percent of Internet users reported searching online for health-care information. [8] Th ey research the best available insurance plans. They investigate their conditions or diseases even before they have official diagnoses. [9] They want to know about the safety and efficacy of potential therapies, and they also want the ability to do a cost/benefit analysis. [10] After all, the health marketplace is premised on the expectation that patients will make informed choices. [11] In fact, of those patients who reported investigating their conditions online, nearly half said that the information they found led them to believe that they needed the attention of a medical professional, and 41 percent indicated that a medical professional confirmed their online self-diagnosis. [12]

[8] Susannah Fox & Maeve Duggan, Health Online 2013, Pew Research Center, http://www.pewinternet.org/2013/01/15/health-online-2013/.

[9] Id.

[10] Sastry Chilukuri et al., A Digital Prescription for Pharma Companies, McKinsey & Co., November 2014, available athttp://www.mckinsey.com/insights/health systems and services/a digital prescription for pharma companies.

[11] Lisa Suennen, Ante Up! Where I'd Place My Healthcare Bets, Venture Valkyrie, http://venturevalkyrie.com/ante-up-where-id-place-my-healthcare-bets/.

[12] Supra note 8.

Patients also increasingly have the ability to access their own health information. [13] Unlike health-care providers who are bound by HIPAA, patients are free to disclose sensitive health information. [14] In the face of patients' willingness to engage in social media, is there a cause for concern regarding what might be done with health information that they themselves provide on these platforms?

[13] 45 C.F.R. § 164.524; 42 C.F.R. 493.1291(l).

[14] See e.g. American Academy of Family Physicians, Confidentiality, Patient/Physician, http://www.aafp.org/about/policies/all/patient-confidentiality.html; Centers for Medicare & Medicaid Services, Are You a Covered Entity?, http://www.cms.gov/Regulations-and-Guidance/HIPAA-Administrative-Simplification/HIPAAGenInfo/AreYouaCoveredEntity.html.

Those with medical conditions appear to be particularly vulnerable. In a recent Institute of Medicine survey of social media users with medical conditions:

- 94 percent said they would be willing to share data about their health to help doctors improve care;
- 92 percent supported sharing their health data anonymously to assist researchers to learn more about their disease;
- 84 percent said they would be willing to share their information with drug companies to help them make products safer; and
- 78 percent said they would share information to let drug companies learn about their disease.

A willingness to share information exists, despite beliefs that personal health data might be used without patient permission, potentially to deny health-care benefits. [15]

[15] Francisco Grajales et al., Social Networking Sites and the Continuously Learning Health System: A Survey, Institute of Medicine of the National Academies Discussion Paper, Feb. 4, 2014, available athttp://www.iom.edu/~/media/Files/Perspectives-Files/2014/Discussion-Papers/VSRT-PatientDataSharing.pdf

Risks of Participation

Consider PatientsLikeMe, which now includes sites for patients with nearly 100 different conditions. [16] Users are explicitly informed via the Privacy Policy that the site is a "sharing" website designed to "create collective knowledge about disease, health, and treatments." [17] Acceptance of the Privacy Policy is a condition of use. Information may be collected and shared with others who are part of the particular disease community, including biographical data, and information about diagnosis, family history, symptoms, treatment, sensor data, lab results and genetic information. [18] Members have the option of restricting access to their data, but only as to certain categories. [19] Generally, members should expect that "every [other] piece of information they submit (even if it is not currently displayed) . . . may be shared . . . ."

[16] PatientsLike Me, Conditions, https://www.patientslikeme.com/conditions; PatientsLikeMe, About Us, http://www.patientslikeme.com/about.

[17] PatientsLikeMe, Privacy Policy, http://www.patientslikeme.com/about/privacy.

[18] Id.

[19] Id. Members may restrict access to their names, e-mail and mailing addresses, passwords, birth dates and private messages.

The site has been proactive about warning its members when a third party inappropriately accesses member profiles. [20] The site also requires that its members agree that their use of the site will be noncommercial in nature, but it retains the ability to share user data with their partners, which include half of the world's 12 largest pharmaceutical companies. [21]

[20] iHealth Beat, 'Scraping' Incident Illustrates Risks for Online Health Data, Oct. 13, 2010, http://www.ihealthbeat.org/articles/2010/10/13/scraping-incident-illustrates-risks-for-online-health-data .

[21] PatientsLikeMe, Terms and Conditions of Use, http://www.patientslikeme.com/about/user_agreement; PatientsLikeMe, Partners: Industry, http://www.patientslikeme.com/about/partners#industry (identifying Abbott, Bristol-Myers Squibb, Genentech (Roche), Merck, Novartis and Sanofi as partners).

Although patient-informed consent must be obtained before researchers are allowed to use the data shared on medical social networking sites, marketers are not bound by such requirements. And social media sites, unlike health-care providers, are not bound by HIPAA to protect information because it is information that is voluntarily shared by patients themselves. Facebook, LinkedIn and Twitter, for example, allow their users the option of adjusting privacy settings, but those settings do not shield a user's information from the site itself. The relevant terms stipulate that the site has broad access to user-posted content, and an explicit sublicense to use any IP. [22] And as it relates to potentially sensitive health information, each social media site may protect patient data differently. Google, for example, prohibits targeted advertising based on "sensitive personal information," which includes "personal information related to confidential medical facts" and "health." [23] Facebook's Data Use Policy, on the other hand, explicitly states that information shared with advertisers includes user page likes on topics such as "health status," but that advertisements to these users may not "assert or imply within the ad content a user's disability or medical condition." [24] This means that despite an individual's intent to hide health-related page likes from their Facebook friends, information about their health status could potentially still be shared with advertisers and their partners.

[22] See e.g., Facebook, Data Policy, https://www.facebook.com/about/privacy/your-info; LinkedIn, User Agreement, http://www.linkedin.com/legal/user-agreement; Twitter, Terms of Service, https://twitter.com/tos.

[23] Google, Privacy & Terms—Key Terms, http://www.google.com/policies/privacy/key-terms.

[24] Facebook, Data Policy, https://www.facebook.com/full_data_use_policy; Facebook, Facebook Advertising Guidelines, https://www.facebook.com/ad_guidelines.php.

Even when a user chooses not to affirmatively share health information, social media sites have the ability to track traffic patterns, monitoring how their users navigate to, from and within their sites, as well as what their users buy and where they are physically located. Collectively, user information has been a gold mine for targeted marketing, which has been the subject of multiple class action suits. Is there any recourse when a social media platform chooses to use patient information in a manner that goes against a patient's wishes? This may turn on whether a patient can successfully challenge the site's Terms of Use (Terms).

In other contexts, social media users have challenged Terms, often unsuccessfully.

Facebook successfully enforced its venue selection clause in a case brought by minors in Illinois. [25] Facebook moved to transfer the case to California based on a forum selection clause in its Terms, which stated that any claim arising out of or relating to the Terms would be resolved exclusively in state or federal court in Santa Clara, Calif., under California law. Plaintiffs argued that the forum selection clause should not be enforced in this instance because they were minors who lacked the capacity to enter into a binding contract. But California law prevents minors from inequitably retaining the benefits of a contract while disclaiming their obligations. [26] In this case, plaintiffs had continued to use their Facebook sites throughout the

litigation. And the forum selection clause was valid because plaintiffs did not show that its enforcement would be unreasonable. All users were on reasonable notice of Facebook's Terms, which were hyperlinked on every page. Moreover, establishing a Facebook account is conditioned on acceptance of the Terms.

[25] *E.K.D. v. Facebook, Inc.*, 885 F. Supp. 2d 894 (S.D. Ill. 2012).

[26] Id. at 899.

The case was subsequently transferred to Facebook's chosen venue. [27] Plaintiffs continued to argue that Facebook's Terms were unenforceable, relying on California Family Code § 6701, under which minors cannot make a contract relating to any personal property not in their immediate possession. Under this theory, plaintiffs' acceptance of Facebook's Terms had created contracts that were void. The statutory language, however, referred to "personal property" that was "tangible," and therefore did not apply to the use of names and pictures on a Facebook page. [28] The contract between plaintiffs and Facebook governed by the Terms was also not voidable. While § 6701 provides that minors may disaffirm a contract, plaintiffs had never expressed an intent to do so. Again, they had continued to use their accounts. [29]

[27] *C.M.D. v. Facebook, Inc.*, No. 3:12-cv-01216, 2014 BL 85230 (N.D. Cal. Mar. 26, 2014).

[28] Id. at *3-4; but see *I.B. v. Facebook, Inc.*, 905 F. Supp. 2d 989 (N.D. Cal. 2012) (holding that plaintiffs had alleged a plausible claim under § 6701 based on minors purchasing Facebook credits through their parents credit or bank accounts).

[29] C.M.D., supra note 28, at *4-5.

Facebook's Terms have also been at issue in cases brought in California. Plaintiffs alleged violations of the Right of Publicity, which prevents the unauthorized commercial use of another's image, likeness or name. [30] In one instance, the claims arose over Facebook's Friend Finder, which Facebook promoted by using its members' names and profile pictures. [31] Facebook moved to dismiss the suit based on its Terms and on a lack of cognizable injury to plaintiffs. The case was dismissed because plaintiffs could not demonstrate that their names and photos ever appeared anywhere that they had not already authorized (i.e. their friends' pages). [32]

[30] See e.g., California Civil Code § 3344.

[31] *Cohen v. Facebook, Inc.*, 798 F. Supp. 2d 1090 (N.D. Cal. 2011).

[32] Id.

Plaintiffs who brought a suit based on Facebook's Sponsored Stories fared a bit better. [33] The accused feature would associate a Facebook user with an advertiser based on the user's actions, such as liking content related to the advertiser, or playing a game on Facebook that included advertiser-related content. In a sponsored story, a user's name and profile picture were juxtaposed with the advertiser and displayed on the user's friends' pages. Facebook again moved to dismiss the suit based on lack of injury to plaintiffs. In this case, though, the court determined that plaintiffs had sufficiently pleaded an economic injury.

[33] *Fraley v. Facebook, Inc.*, 966 F. Supp. 2d 939 (N.D. Cal. 2013).

As Facebook was well aware, there is a property interest in personal endorsements:

- "[N]othing influences people more than a recommendation from a trusted friend."
- "A trusted referral is the Holy Grail of advertising."
- "[M]aking your customers your marketers" is "the illusive (sic) goal we've been searching for." [34]

[34] *Fraley et al. v. Facebook, Inc.*, 830 F. Supp. 2d 785 (N.D. Cal. 2011). Facebook is not alone in recognizing the value of its users' endorsements. LinkedIn's documents reflect that its member base has "grown virally" based on members inviting other members to join and that it has consequently been able to build its brand with "relatively low marketing costs." *Perkins v. LinkedIn Corp.*, No. 5:13-cv-04303, 2014 BL 163436 (N.D. Cal. June 12, 2014).

The court also declined to decide, on a motion to dismiss, whether Facebook's Terms shielded it from liability. [35] The case settled, and Facebook agreed to give its users additional information about—and control over—the use of their names and photos. [36]

[35] Fraley, supra note 34.

[36] *Fraley v. Facebook, Inc.*, No. 3:11-cv-01726, 2012 BL 210317 (N.D. Cal. Aug. 17, 2012).

Aside from the sites themselves, who else might have access to patient health information posted on social media? For starters, anyone else to whom a user has granted access, whether it be a different social media site, or a third-party app developer. But also potentially anyone to whom a user's connections have granted access. There's the rub. A person's privacy on social media might depend on the good judgment of 780 of her closest friends. Some have found this out the hard way. For example, Snapchat reported a leak of hundreds of thousands of photos, many of which were probably only sent in the first place because their senders expected them to disappear within seconds of receipt. [37] Turns out there are third-party apps—not endorsed by Snapchat—that let recipients save photos. PatientsLikeMe also faced scrutiny when it discovered that Nielsen Co. was "scraping," or copying, personal data from private bulletin boards and chat rooms where users shared information about medical conditions. PatientsLikeMe identified and blocked the security breach, but it's clear that there is a robust market for personal health data. Moral of the story? End runs can be done around privacy safeguards on social media platforms, sometimes without a user's permission or knowledge. [38]

[37] Ruth Reader, Snapchat Blames Users of 'Illegal Third Party Apps' for Nude Photo Hack, VentureBeat, Oct. 10, 2014, available at http://venturebeat.com/2014/10/10/snapchat-responds-to-nude-photo-hack-passes-blame-to-users/; Press Release, FTC, Snapchat Settles FTC Charges That Promises of Disappearing Messages Were False (May 8, 2014), available at http://www.ftc.gov/news-events/press-releases/2014/05/snapchat-settles-ftc-charges-promises-disappearing-messages-were; Davey Alba, Snapchat Hands-on: Send Photos Set to Self-Destruct, Laptop, May 16, 2012, available at http://blog.laptopmag.com/hands-on-with-snapchat-send-photos-set-to-self-destruct.

[38] See e.g. Privacy Rights Clearinghouse, Fact Sheet 35: Social Networking Privacy: How to Be Safe, Secure and Social, https://www.privacyrights.org/social-networking-privacy-how-be-safe-secure-and-social.

Patient health information may also be gathered and disclosed during litigation, as social media content can be subpoenaed. Requests may or may not be narrowly tailored in civil actions, [39] and may or may not be supported by probable cause in criminal cases. [40] And, regardless, social media providers may be willing to share information instead of fighting a request. Facebook, for example, produced at least some information more than 80 percent of the time in response to the over 12,000 requests it received in a six-month period. This corresponded to requests for information about over 18,000 users. [41]

[39] *Brogan v. Rosenn, Jenkins & Greenwald, LLP*, 28 Pa. D. & C.5th 553 (Pa. Ct. Com. Pl. 2013); *Patterson v. Turner Constr. Co.*, 88 A.D.3d 617 (N.Y. App. Div. 2011).

[40] *In re Search of Info. Associated with the Facebook Account Identified by the Username Aaron.Alexis*, 21 F. Supp. 3d 1 (D.D.C. 2013).

[41] Facebook, Government Requests Reports, United States Law Enforcement Requests for Data, July-December 2013, https://govtrequests.facebook.com/country/United%20States/2013-H2.

While Facebook users are generally known based on the content of their pages, other platforms are intended to allow users a degree of anonymity, such as Yelp, which is designed to let consumers anonymously review local businesses. [42] In response to a rash of negative reviews that it could not correlate with actual customers, a carpet cleaning company subpoenaed the identities of the reviewers to support an eventual defamation claim. [43] Yelp unsuccessfully resisted the request. Freedom to speak anonymously is not unlimited, and protections do not extend to false speech. In addition, the party seeking to enforce the subpoena had complied with the state's unmasking statute. [44]

[42] Yelp, About Us, http://www.yelp.com/about.

[43] *Yelp, Inc. v. Hadeed Carpet Cleaning, Inc.*, 752 S.E.2d 554 (Va. Ct. App. 2014).

[44] *Hadeed Carpet Cleaning, Inc. v. John Doe #1*, 86 Va. Cir. 59 (Va. Cir. Ct. 2012); *Yelp*, supra note 43; and see Virginia Code § 8.01-407.1.

The scope of the risks of government-compelled disclosures is perhaps best illustrated by the Lavabit case. Lavabit was an encrypted e-mail service once used by former government contractor Edward Snowden. In its efforts to apprehend Snowden, the FBI first requested targeted billing and subscriber information but then expanded its requests to include Lavabit's encryption keys. [45] The problem? This would have given the government not only the ability to trap and trace the Snowden account but also to review the e-mails of each of the other 410,000-some subscribers. [46] Imagine the impact of a similar request to Facebook. In theory, the government could obtain private messages sent between any of Facebook's users, or more than one-sixth of the world's population.

[45] See *United States v. Lavabit*, No. 1:13 EC297 (E.D. Va. June 28, 2013), available at http://www.clearinghouse.net/detail.php?id=13002.

[46] Ladar Levison, Secrets, Lies and Snowden's Email: Why I Was Forced to Shut Down Lavabit, Guardian, May 20, 2014, available at http://www.theguardian.com/commentisfree/2014/may/20/why-did-lavabit-shut-down-snowden-email.

Privacy concerns—in particular regarding sensitive information about patient health on social media—are only likely to increase over time. The tradeoff, though, may be significant benefits to patients in the long run. It remains to be seen whether relationships can be effectively built over social media, to allow stakeholders to take advantage of the "super-convergence taking place between the digital revolution and health." [47] Or whether a social media platform that allows patients to come together in cyberspace can also be used to align patient groups with the relevant industry interests, [48] in such a way that patient interests are best served.

---

[47] Stephen Davies, Fifteen Influencers Shaping Digital Health in 2014, Bionicly, Mar. 31, 2014, available at http://bionicly.com/fifteen-influencers-shaping-digital-health-in-2014/.

[48] PatientsLikeMe, About Us, http://www.patientslikeme.com/about

---