Santa Clara High Technology Law Journal

Volume 32 | Issue 1 Article 3

12-11-2015

Direct Digital Engagement of Patients and Democratizing Health Care

Dov Greenbaum

DIRECT DIGITAL ENGAGEMENT OF PATIENTS AND DEMOCRATIZING HEALTH CARE

Dov Greenbaum JD, PhD, CIPP/E[†]

Smartphones and social media have changed the way we integrate technology into our daily lives, and this is quickly bleeding into diverse medical fields. Many social media sites provide specialty forums for the sick to interact with their peers. Unfortunately, these sites are mostly unregulated environments where advertisers can prey on the desperate but unwary, people can provide their unwarranted but seemingly authoritative medical opinions, and clinicians can troll for cohorts for their studies. These sites also encourage users to share personal and private medical information; oftentimes that medical information implicates not only the immediate patient, but also her extended family members who might be similarly experiencing, but more privately, the same or similar medical conditions.

Just like social media brings medical consultancy to the masses, smartphones have brought medical diagnostics to just about anyone who can download a mobile device software application (app). Diagnostic and other medical apps often take advantage of the ever-shrinking size of wearable technologies, as well as advances in computing that can offer doctors, patients, and third parties powerful medical tools on their portable computing devices.

The FDA has provided little to no guidance in the Wild West of patient related social media sites. Although it has issued voluntary guidelines for apps intended to diagnose, treat, or prevent diseases many questions remain unanswered. Without clear rules for these relatively new classes of medical devices, and with the threat of regulatory and monetary repercussions for app developers, the FDA may be chilling development of new and useful medically related applications.

Both patient-oriented social media sites and many mobile medical applications (MMAs) are particularly useful and relevant for

---

[†]Assistant Professor, Molecular Biophysics and Biochemistry, Yale University Director, The Zvi Meitar Institute for Legal Implications of Emerging Technologies, Radzyner Law School, Interdisciplinary Center, Herzliya.

the growing class of chronically ill patients. While the potential for heavy-handed regulation of MMAs may chill development in this area and hurt this aforementioned population, the lack of any oversight in patient oriented social media sites may also potentially harm this demographic by not enforcing any filter to a largely lay and desperate population.

This paper will provide brief reviews of the state of the art for these medically related technologies and review the regulatory and legal aspects of these similar but distinct technologies. The paper will suggest both a hybrid regulatory and technological solution for MMAs and a mostly-regulatory solution for policing patient oriented social media sites. These proposed rules will also take into account related issues such as evolving social norms, including the rapid rise of the quantified-self-trend and changes in perceptions of privacy.

TABLE OF CONTENTS

INTRODUCTION

Historically, the Internet and related technologies helped to democratize many aspects of society. This was, and continues to be the case with healthcare. Traditionally, medicine was a paternalistic profession that actively promoted God-complexes amongst its practitioners.[1] These and other high barriers to entry limited the practice of medicine and the development of medical devices to the professionals and to corporations with, or with access to, deep pockets.

Now, anyone who can program a smartphone or tablet application (app) can potentially produce a medical device. Similarly, social media sites aimed particularly at patient populations have empowered patients to help each other and provide additional important care and support, and perhaps surprisingly, useful clinical data. Both concurrent advances in the democratization of health care have the potential to provide substantial benefit. Both, however, also raise a number of serious concerns.

The first part of this paper will suggest a less nuanced and more novel approach to mobile health (mHealth) taxonomy than predecessor papers. This relatively simple approach will be dictated principally by the goal of promoting innovation without jeopardizing safety. This paper argues that under the current and proposed regimes, innovation is not promoted[2] and safety is actually jeopardized.

The second part of the paper will provide arguments as to why even those applications that taxonomically typically fall in what should be an unregulated group of apps really require a hybrid regulatory and technological solution to promote innovation while simultaneously helping and protecting an ever growing demographic.

In the third section, this paper will segue to social media sites aimed at patient subgroups, describing and defining them in detail. The fourth section will raise real and relevant concerns with regard to patient oriented social media sites and suggest a mostly regulatory fix. The final section will provide conclusions.

Notably, this paper hopes to be ahead of the curve regarding the issues raised. As such, data relating to some of the concerns described

---

1. Maureen Dowd, *Decoding the God Complex*, N. Y. TIMES (Sept. 28, 2011), *available at* http://www.nytimes.com/2011/09/28/opinion/dowd-decoding-the-god-complex.html.

2. Marsha Blackburn, et al., Letter From Congressional Representatives to the Food & Drug Admin. and the Fed. Trade Comm'n, U.S. CONGRESSMAN MARSHA BLACKBURN (Apr. 3, 2012), http://blackburn.house.gov/uploadedfiles/letter_from_congress_to_fda_and_fcc__3apr2012.pdf.

herein may be sparse at best.

I. MOBILE MEDICAL APPLICATIONS

Under Section 201 of the Federal Food, Drug, and Cosmetic Act, a device is "an instrument, apparatus, implement, machine, contrivance, implant, in vitro reagent, or other similar or related article, including any component, part, or accessory, which is... intended for use in the diagnosis of disease or other conditions, or in the cure, mitigation, treatment, or prevention of disease, in man or other animals."[3] The U.S. Food and Drug Administration (FDA) has, on a number of occasions, decided that the "intended use clause" includes software; for example, mobile medical applications (MMAs) fall under FDA purview as medical devices.[4,5]

The relatively recent term "mHealth" relates to both mobile health portable electronics software applications and related and/or unrelated appliances.[6] This paper focuses on the former—mobile medical applications (MMAs) in FDA parlance. Their closely related counterparts, mobile health applications (MHAs),[7] will be subsumed under the MMA heading. Currently, most MMAs are classified as Class II devices under current FDA guidelines, i.e., "higher risk devices than Class I that require greater regulatory controls to provide reasonable assurance of the device's safety and effectiveness."[8]

---

3. 21 U.S.C. § 321(h) (2012).

4. U.S. Food & Drug Admin., *Mobile Med. Applications: Guidance For Indus. & FDA Staff*, U.S. FOOD AND DRUG ADMIN., (Feb. 9, 2015), http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM263366.pdf.

5. Suzan Onel, *Where the "App" World and FDA Collide: Current Status of the FDA's Regulation of Medical Device Software and Mobile Medical Apps*, *in* INSIDE THE MINDS, RECENT DEVS. IN FOOD & DRUG LAW 153, 155 (2014), http://www.klgates.com/files/Publication/7642d9b2-62b4-45ff-bf9e-7aa2ad4a7496/Presentation/PublicationAttachment/af8747a0-a280-4d16-8f8c-7b4a48de30a0/Inside_the_Minds_Onel_Chapter.pdf

6. *See* Anne Marie Helm & Daniel Georgatos, *Privacy and mHealth: How Mobile Health "Apps" Fit Into a Privacy Framework Not Limited to HIPAA*, 64 SYRACUSE L. REV. 131, 134 (2014), for a definition of mHealth ("[W]hen a provider of healthcare services uses connected and interactive mobile computing4 to produce, access, transmit, or store data for the provision of healthcare services to patients, or when a patient or consumer uses connected and interactive mobile computing to produce, access, transmit, store, or otherwise share data for a health-related purpose.").

7. Ceara Treacy et al., *Mobile Health & Med. Apps: Possible Impediments to Healthcare Adoption*, *in* PROC. OF THE SEVENTH INT'L CONF. ON EHEALTH, TELEMEDICINE, & SOCIAL MEDICINE 199, 199 (Marike Hettinga et al. eds., 2015).

8. U.S. Food & Drug Admin., *What Does it Mean for FDA to "Classify" a Medical Device?*, ABOUT FDA (Dec. 28, 2015), *available at* http://www.fda.gov/AboutFDA/Transparency/Basics/ucm194438.htm.

There has been a rapid growth of health-related applications for online platforms.[9] According to at least one study, by 2015 there were over 165,000 mobile health apps available for users to download.[10] According to another study, the market for mHealth apps will reach $26 billion globally by 2017.[11] Further, another recent survey suggests that at least 10% of the US population have already downloaded an mHealth application and another 46% would be interested in using the technology to monitor and manage health vitals and other health-related data.[12]

Actual efforts to track the types of mHealth apps available on the myriad of mobile platforms available to users today, estimated at over 40,000,[13] including smartphones, tablets, phablets and the like, seem reminiscent (in retrospect) of the sad efforts to catalogue the internet in the early days of the World Wide Web. With development of mHealth apps rapidly increasing, and with new apps appearing almost daily and older apps falling out of use, these efforts seem, by their very nature, Sisyphean.

These impressive numbers notwithstanding, the medical community still knows very little about the uptake and overall actionable usage of mHealth despite the large number of studies in the field.[14]

In general, these health-related applications for mobile technology fall under the rubric of Health IT. Under current law, three "agencies," including: the Food and Drug Administration (FDA), the Office of the National Coordinator for Health Information Technology (ONC) and the Federal Communications Commission

---

9. Eric Topol, *The Future of Medicine Is in Your Smartphone*, WALL ST. J. (Jan. 9, 2015), *available at* http://www.wsj.com/articles/the-future-of-medicine-is-in-your-smartphone-1420828632.

10. IMS Institute, *Patient Adoption of mHealth* Use, IMS HEALTH (Sept. 2015), available at http://www.imshealth.com/en/thought-leadership/ims-institute/reports/patient-adoption-of-mhealth#ims-form.

11. Ralf-Gordon Jahns, *The Market for mHealth App Services Will Reach $26 Billion by 2017,* RESEARCH2GUIDANCE (2015), *available at* http://www.research2guidance.com/the-market-for-mhealth-app-services-will-reach-26-billion-by-2017.

12. Deloitte, *mHealth: A Check-Up on Consumer Use*, DELOITTE, http://www2.deloitte.com/content/dam/Deloitte/us/Documents/life-sciences-health-care/us-chs-mhealth-infographic.pdf.

13. Scott Rupp, *mHealth Stats: Mobile Apps, Devices and Solutions*, ELEC. HEALTH REPORTER (Dec. 10, 2015), *available at* http://electronichealthreporter.com/mhealth-stats-mobile-apps-devices-and-solutions/.

14. Mark Tomlinson et al., *Scaling Up mHealth: Where is the Evidence?*, 10 PLOS MED. 1 (2013).

(FCC), were recently tasked with determining a "proposed strategy and recommendations on an appropriate, risk-based regulatory framework pertaining to health information technology, including mobile medical applications, that promotes innovation, protects patient safety, and avoids regulatory duplication."[15] In addition, the Federal Trade Commission (FTC) has been cracking down on mHealth apps.[16] For example, the FTC recently fined companies with apps that misrepresent their medical abilities, e.g., the ability to detect cancers.[17]

This work will focus particularly on the FDA, which has a clear regulatory authority over software related to medical devices.[18] According to the most recent list of FDA guidance priorities, the agency may choose to reevaluate its role in medical software, perhaps in light of congressional efforts to cabin it.[19]

However, thus far, the FDA has unreservedly failed in its review of MMAs. On average, the FDA takes 67 days to review a MMA; by this point, the app has often been updated and likely changed such that the initial product no longer resembles the app submitted for review.[20] Moreover, only a minute percentage of the available apps have even been reviewed by the FDA; the majority of them have been classified as Class II medical devices.[21]

Whereas most analyses of the current state of affairs for health-related apps tend to fault the FDA's guidance documents for any

---

15. FDA SAFETY & INNOVATION ACT (FDASIA), Pub. L. No. 112-144, § 618, 126 Stat. 993 (2012).

16. *See, e.g.*, FTC Watch, *More Consumer Protection Action on the Way at the FTC*, FTC WATCH ISSUE NO. 823 (Feb. 14, 2013) *available at* http://ftcwatch.com/series/823.

17. Federal Trade Commission, *FTC Cracks Down on Marketers of "Melanoma Detection" Apps*, PRESS RELEASES (Feb. 23, 2015), *available at* https://www.ftc.gov/news-events/press-releases/2015/02/ftc-cracks-down-marketers-melanoma-detection-apps.

18. Richard A. Merrill, *The Architecture of Government Regulation of Medical Products*, 82 VA L. REV. 1753 (1996).

19. *See, e.g.*, Darius Tahir, *FDA Puts Interoperability Guidance on Back Burner*, MODERN HEALTHCARE (Jan. 9, 2015), *available at* http://www.modernhealthcare.com/article/20150109/NEWS/301099953.

20. Greg Slabodkin, *FDA's Bakul Patel: For Mobile Medical Apps, Patient Safety First*, FIERCE MOBILE HEALTHCARE (May 23, 2013), *available at* http://www.fiercemobilehealthcare.com/story/fdas-bakul-patel-mobile-medical-apps-patient-safety-first/2013-05-23.

21. John Avellanet, *Majority of Mobile Health Apps Class II Devices for FDA*, COMPLIANCE ZEN (July 2013), *available at* http://www.compliancezen.com/compliance_zen/2013/07/majority-mobile-health-apps-class-ii-devices-fda.html; *see also* Ting-Yu Wang et al., *mAuditor: Mobile Auditing Framework for mHealth Applications*, *in* PROC. OF THE 2015 WORKSHOP ON PERVASIVE WIRELESS HEALTHCARE 7, 7 (Emmanuel Baccelli et al. eds, 2015).

number of limitations, omissions and other errors, this paper will argue that much of the proposed FDA regulation of mHealth should be done away with entirely, with any regulation limited to only a small subset of apps. Under this initial proposal most consumer apps, arguably the bulk of the current catalogue of MMAs, would remain essentially unregulated under the FDA.

To some degree, this is the goal of the Preventing Regulatory Overreach To Enhance Care Technology (PROTECT) Act of 2014[22] which ultimately was not passed.[23] As per US Senator Deb Fischer's (R-Neb) office:

Under current law, the FDA can use its definition of a medical device to assert broad regulatory authority over a wide array of low-risk health IT, including mobile wellness apps, scheduling software, and electronic health records. The PROTECT Act gives clarity to FDA's regulatory process to focus on products that pose a legitimate risk to human health. This more effective, risk-based framework boosts patient safety by prioritizing FDA's attention to technologies that pose the greatest health risk. It also protects low-risk health IT from unnecessary regulatory burdens that stifle opportunities for job creation, innovation, and improved care.[24]

Somewhat counterintuitively to the MMA arguments, this paper will also argue that social media sites focused on patient groups ought to be more regulated, albeit perhaps not by the FDA. This might even go against conventional wisdom at the FDA, which after years of delays,[25] effectively dropped social media from its 2011 guidance agenda,[26] but later re-included it.[27]

---

22. THE PROTECT ACT, S. 2007, 113th Cong. (as introduced, Feb. 10, 2014), *available at* https://www.govtrack.us/congress/bills/113/s2007/text/.

23. *Id.*

24. Angus King, *King, Fischer Introduce Legis. to Protect Jobs, Prevent Overregulation in Growing Health IT Industry,* ANGUS KING UNITED STATES SENATOR FOR MAINE, (Feb. 10, 2014), *available at* http://www.king.senate.gov/newsroom/press-releases/king-fischer-introduce-legislation-to-protect-jobs-prevent-overregulation-in-growing-health-it-industry/.

25. *Breaking – Its Official – FDA Delaying Social Media Guidance Until at Least Q1 2011*, EYE ON FDA (Dec. 2010), *available at* http://www.eyeonfda.com/eye_on_fda/2010/12/breaking-its-official-fda-delaying-social-media-guidance-until-at-least-q1-2011.html.

26. *FDA Drops Social Media from Its 2011 Guidance Agenda*, PHARMA MARKETING BLOG (June 1, 2011), http://pharmamkting.blogspot.com/2011/06/fda-drops-social-media-from-its-2011.html.

27. U.S. Food & Drug Admin., *Guidance Agenda: New & Revised Draft Guidances CDER is Planning to Publish During Calendar Year 2016*, U.S. FOOD AND DRUG ADMIN. (Jan. 22, 2016), http://www.fda.gov/downloads/Drugs/GuidanceComplianceRegulatoryInformation/Guidances/UCM417290.pdf

A. MMA Taxonomy

Taxonomies have been developed in an attempt to catalogue the wide array of potentially regulatable mobile medical applications,[28] including a taxonomy by the FDA itself that confusingly makes an important practical distinction between those apps that pose "a risk to patients" and those apps that "pose a *low* risk to patients," a distinction poorly clarified in the FDA's appendix to their guidance documents.[29]

The Food and Drug Administration Safety and Innovation Act (FDASIA) "expands the FDA's authorities and strengthens the agency's ability to safeguard and advance public health."[30] Included in this authority, a workgroup was " charged with providing expert input on issues and concepts identified by the Food and Drug Administration (FDA), Office of the National Coordinator for Health IT (ONC), and the Federal Communications Commission (FCC) to inform the development of a report on an appropriate, risk-based regulatory framework pertaining to health information technology including mobile medical applications that promotes innovation, protects patient safety, and avoids regulatory duplication."[31] But even the FDASIA working group's more fleshed-out stratification of risk does not take into account many of the concerns raised herein with regard to concerns with MMAs.[32]

While some of these taxonomies attempt to place each individual type of application into its most relevant and distinctive classification, this paper proposes perhaps a crude and consequentially more useful taxonomy.

A binary taxonomy is particular useful, if not actually necessary, and is even more simplistic than the current FDA April 2014

---

28. *See, e.g.*, Miloslava Plachkinova et al., *A Taxonomy of mHealth Apps—Security and Privacy Concerns*, *in* PROC. OF THE 2015 48TH HAW. INT'L CONF. ON SYS. SCIENCES (HICSS) 3187, 3187 (Tung X. Bui et al. eds., 2015).

29. U.S. Food & Drug Admin., *supra* note 4, at 23.

30. U.S. Food & Drug Admin., *Food and Drug Administration Safety and Innovation Act*, REGULATORY INFORMATION (Oct. 6, 2015), *available at*http://www.fda.gov/RegulatoryInformation/Legislation/SignificantAmendmentstotheFDCAct/FDASIA/ucm20027187.htm.

31. HealthIT.gov, *FDASIA*, HEALTHIT.GOV (June 17, 2015), *available at* https://www.healthit.gov/facas/health-it-policy-committee/hitpc-workgroups/fdasia.

32. Sarah P. Slight & David W. Bates, *A Risk-Based Regulatory Framework for Health IT: Recommendations of the FDASIA Working Group*, 21 J. AM. MED. INFORMATICS ASS'N, No. e2, 2014, at e181-4.

recommendations.[33] Many software developers in the mHealth field may simply be startups[34] that are not as savvy to FDA regulation and oversight as their more experienced medical device manufacturer counterparts; as such they may be discouraged from innovating in this area if they lack the ability to relatively easily assess their regulatory environment from the outset.[35] This is particularly problematic given that in many cases the FDA has reverted to applying its standard medical device methodologies in assessing MMAs.[36]

The goal of this effort would be to simplistically divide apps into manageable categories that reflect the subsequent nature of their regulation. The more basic the divisions, the easier they are to apply, particularly for the uninitiated. And the less likely that the uninitiated startup innovators in this field will be confused, the less likely innovation will be chilled. For example, given that Class II devices face increased regulations and costs of doing business,[37] MMA developers will want to know beforehand, or before huge expenses have been sunk, whether they fall into a class associated with high costs or a class associated with low regulatory costs.

mHealth is particularly being pursued aggressively by startups that are relatively FDA-naïve. For example, venture capital investors have pumped more than a quarter billion dollar in the start of 2013 into mHealth.[38] Even with the need for regulatory oversight, the FDA should be careful to promote rather than inhibit innovation in this area

---

33. U.S. Food & Drug Admin., *FDASIA Health IT Report*, ABOUT FDA (April 21, 2014), *available at* http://www.fda.gov/AboutFDA/CentersOffices/OfficeofMedicalProductsandTobacco/CDRH/CDRHReports/ucm390588.htm.

34. *See, e.g.,* MHEALTH STARTUPS, https://angel.co/mhealth (last visited Jan. 10, 2016); MHEALTH, https://www.crunchbase.com/category/mhealth/a3b491d88d66b566a059c14322895d77 (last visited Jan. 10, 2016); MOBIHEALTHNEWS, http://www.mhealthnews.com/blog/42-startups-cusp-mhealth-innovation (last visited Jan. 10, 2016); ROCK HEALTH https://rockhealth.com/reports/digital-health-2015-midyear/ (last visited Jan. 10, 2016);

STARTUP HEALTH INSIGHTS https://www.startuphealth.com/content/insights-2015q2 (last visited Jan. 10, 2016).

35. Robert L. Garrie & Pamela E. Paustian, *mHealth Regulation, Legislation, and Cybersecurity*, in MHEALTH 45, 45 (Springer US, 2014).

36. Vanessa Coleman, *FDA Approved?: Examining the FDA's Approach to Mobile Medical Apps and its Sufficiency*, LAW SCHOOL STUDENT SCHOLARSHIP SETON HALL LAW (2015), http://scholarship.shu.edu/cgi/viewcontent.cgi?article=1681&context=student_scholarship.

37. Avellanet, *supra* note 21.

38. Nanette Byrnes, *Mobile Health's Growing Pains*, MIT TECH. REVIEW (July 21, 2014), *available at* http://www.technologyreview.com/news/529031/mobile-healths-growing-pains/.

as it has already been shown that mHealth apps are beneficial in the health care environment, allowing for more rapid and accurate health care decisions by health care providers.[39]

To this end, this paper argues for a dualistic regulatory oversight test. An application necessitates some form of regulatory oversight by the FDA when: (1) a mHealth app is configured and/or otherwise designed to be used in a clinical environment [e.g., in conjunction with electronic health records (EHRs) such as in a doctor's office, ambulance, clinic, or hospital] and (2) that application uses one or more sensors (onboard and/or external) to perform a calculation based on data obtained in real or near-real-time from the patient, her hospital bed or other patient related data. This is slightly broader than the FDA's own regulatory system which, while seeming very broad in applying its oversight to mainly those apps "whose functionality could pose a risk to patient safety if the [MMAs] were not to function as intended,"[40] is in practice very narrow. The extent of that regulatory control should be related to the destined usage of the application and the nature of the application. The regulation of these apps should include a standardization of data collection and storage, as well as standardized application program interfaces (APIs), so that different apps can easily and coherently communicate with each other.

All other mHealth apps, such as consumer directed apps, do not need any regulatory oversight whatsoever by the FDA. However, they must be clearly marked as being recreational/non-clinical to ward off this proposed governmental oversight. In this sense, the application must also not make any clinical claims related to its utility, or market itself as such. This clear demarcation might include a clickwrap agreement, and/or a perpetual clickwrap feature in which the user must click through a simple statement noting the limited (i.e. recreational) use of the application every time the user employs the application. This suggestion follows conventional wisdom wherein nearly a third of correspondents to a 2013 Deloitte survey believed that mobile applications are likely to have potential errors.[41] And in

39. Mirela Prgomet et al., *The Impact of Mobile Handheld Technology on Hospital Physicians' Work Practices and Patient Care: A Systematic Review*, 16 JOURNAL OF THE AM. MED. INFORMATICS ASS'N 792, 792 (2009); Lex van Velsen et al., *Why Mobile Health App Overload Drives Us Crazy, and How to Restore the Sanity*, MED. INFORMATICS & DECISION MAKING, NO. 23, 2013, at 1 (2013).

40. U.S. Food & Drug Admin., *supra* note 4, at 4.

41. Deloitte, *supra* note 12.

any event, it would be unfeasible for any government organization to effectively police and regulate the growing ranks of mHealth apps, particularly in light of the above concerns. Moreover, in addition to the errors, there are other legitimate health-related concerns for consumer-facing applications, such as over-reliance on non-human analysis and the inability of many of the applications to find secondary medical problems that might otherwise be discovered in a face-to-face doctor visit.[42]

The types of apps that would fall under the regulation-free designation would include many of those that are, or could be, regulated by the FDA as proposed under their guidance documents.

B. Why MMAs Should Not Be Marketed As Medical Devices

Not only must mHealth applications for use in clinical settings be regulated, they actually ought to be regulated *and* consistently monitored. The nature of the technology demands such oversight. For instance, consider the following scenario. There are hundreds of millions of smartphones in the world with a myriad number of distinct and diverse models running a wide variety of operating systems and their respective versions. Data from 2013 suggests that only about 4% of all Android mobile phones and devices were running the most up-to-date version of the operating software; the rest were running any number of other variations, which does not include the multitude of free and/or otherwise applications on these devices that alter basic operating aspects of the phone either unintentionally or even maliciously.[43]

Each smartphone contains a number of sensors, i.e., a sensor being something that measures a physical quantity and converts that physical quantity into a digital or analog signal that can be read by the onboard processing hardware, including those that measure motion, orientation, and environmental conditions. These sensors can be hardware, software, or a hybrid of the two.

"Hardware-based sensors are physical components built into a handset or tablet device. They derive their data by directly measuring specific environmental properties, such as acceleration, geomagnetic field, strength, or angular change. Software-based sensors are not

---

42. Stephen McInerney, *Can You Diagnose Me Now? A Proposal to Modify the FDA's Regulation of Smartphone Mobile Health Applications with a Pre-Market Notification and Application Database Program*, 48 U. MICH. J.L. REFORM 1073, 1079 (2015).

43. MARC GOODMAN, FUTURE CRIMES: EVERYTHING IS CONNECTED, EVERYONE IS VULNERABLE AND WHAT WE CAN DO ABOUT IT 107 (2015).

physical devices, although they mimic hardware-based sensors. Software-based sensors derive their data from one or more of the hardware-based sensors and are sometimes called virtual sensors or synthetic sensors. The linear acceleration sensor and the gravity sensor are examples of software-based sensors."[44]

Motion sensors can include gravity sensors, accelerometers, linear acceleration sensors, rotational vector sensors tracking chips (which can distinguish between a phone holder's walking and driving) and gyroscopes. Orientation sensors can include geomagnetic field sensors, positional sensors, global positioning sensors and the like. Environmental sensors can include infrared, force, ambient air temperature sensors and local air pressure sensors. Additionally, environmental sensors can include proximity, illumination, and humidity sensors. Also included in the group of environmental sensors are photometers, barometers, and thermometers.[45]

Other onboard sensors include microphones and pedometers. The increasingly powerful cameras on smartphones are also useful sensors. Many recent models of smartphones also include fingerprint sensors. Some phones even include sensors that can detect harmful radiation. All in all, these sensors can have various distinct operating parameters including different ranges, power requirements, and varied resolution abilities.

Each smartphone model could potentially have a distinct set of sensors and each of these sensors may interact differently (albeit sometimes minimally so) with the wide variety of operating systems and their respective versions: "**Note:** Android does not require device manufacturers to build any particular types of sensors into their Android-powered devices, so devices can have a wide range of sensor configurations."[46]

Downloaded software, not to mention malicious code, could affect the way sensors read physical quantities. In some examples, this affect could be imperceptible yet nevertheless actionable.

Additionally, even smartphone protective cases may affect the onboard sensors, if only minimally, not to mention the various bumps and bangs typical of the daily wear and tear on a smartphone. For example, it has been shown that something as seemingly benign as

---

44. SENSORS OVERVIEW, http://developer.android.com/guide/topics/sensors/sensors_overview.html (last visited Oct. 24, 2015).

45. *Id.*

46. *Id.*

prolonged exposure to refrigerator magnets can decalibrate some smartphone magnetometers.

Given all this variability it would seem nearly impossible to design a reliable, accurate, and medically appropriate consumer oriented mHealth app that could take into account, in its assessment of the patient's health, all of the potential variability associated with the sensors and the resulting data they collect. Uncalibrated, smartphone sensors are often error prone and unreliable for a number of tasks.[47, 48] Even with minute changes, we run the risk of potentially drastically different and potentially misguided results that could wrongly direct an individual concerned as to their health.

To deal with all of this uncertainty some have suggested the mHealth applications rely only on a subset of sensor data from smartphones such as subset of sensors that are onboard trusted sensors, e.g., "sensors whose readings cannot be easily manipulated by the smartphone's OS or by applications."[49] However, these trusted sensors may represent only a small subset of onboard, useful, and/or relevant sensors.

Under any regulatory regime, the reliability of the application might need to be reassessed after each and every operating system upgrade or patch, or application software upgrade, and for each new model and their respective subtypes. For these reasons alone, it would seem to be prudent for the FDA to keep a close regulatory eye on mHealth apps to confirm that each one is constantly updated to account for changing technology. But, for these same reasons, it would be nearly impossible for the FDA to keep tabs on all of the direct to consumer products and all their iterations that might be developed to deal with all of the software and hardware changes and versions.

"The FDA is woefully understaffed and under-resourced to oversee these things, particularly given the number of the thousands of apps that are [most likely] under FDA's jurisdiction."[50] This is

---

47. Antonio Villasante & Cristina Fernandez, *Measurement Errors in the Use of Smartphones as Low-Cost Forestry Hypsometers*, 48 SILVA FENNICA, NO. 5:1114, 2014, at 1.

48. JEFFREY R. BLUM ET AL., *Smartphone Sensor Reliability for Augmented Reality Applications, Mobile and Ubiquitous Systems*, *in* MOBILE & UBIQUITOUS SYSTEMS: COMPUTING, NETWORKING, AND SERVICES, 127-38 (2013).

49. Alec Wolman et al., *Using Trusted Sensors to Monitor Patients' Habits*, MICROSOFT RESEARCH (2010), http://research.microsoft.com/en-us/um/people/alecw/healthsec-2010.pdf.

50. Bahar Gholipour, *Should You Trust Health Apps on Your Phone?* LIVE SCIENCE (July 25, 2014), *available at* http://www.livescience.com/47021-health-apps-fda-regulation.html

compounded by the sheer number of users who are likely to use this software, with some estimates suggesting that there could be more than one and half billion users worldwide by 2018.[51] With such staggering numbers, and the ability to easily provide hundreds of thousands of copies of software to patients, even minor missteps can have huge repercussions. In light of the common conception that the FDA is unequipped and understaffed for these sorts of regulatory oversight projects, some in Congress have suggested that mHealth ought to be excluded from the FDA's purview.[52,53]

C. Regulatory Oversight Should Be Constrained In Most Situations

The quantified-self movement uses a lot of non-standardized consumer technologies to quantify aspects of our lives, including products like Fitbit, and Apple Health. In addition to the lack of standardization, many of these products vary in their ability to accurately measure different health-related data.[54, 55] These technologies and their associated apps are, in many respects, similar to MMAs, although arguably distinct in the nature of the analysis of the data collected by these technologies, and/or the stated uses of that data or analyzed data[56]

However, without the ability to provide an absolutely clear demarcation where quantified self apps end and mHealth apps begin a standardized definition of what is and what isn't a consumer mHealth application is likely to remain elusive. Nevertheless, both types of software apps aimed at the consumer market should be able to escape

---

(quoting a health law expert, Nathan Cortez, associate professor of law at Southern Methodist University Dedman School of Law in Dallas, Texas).

51. Mary Beth Hamel et al., *FDA Regulation of Mobile Health Technologies*, 371 NEW ENG. J. MED. 372, 372-79 (2014).

52. The Sensible Oversight for Technology Which Advances Regulatory Efficiency Act of 2013 (SOFTWARE Act), H.R. 3303, 113th Cong. (1st Sess. 2013).

53. The Preventing Regulatory Overreach to Enhance Care Technology Act of 2014 (PROTECT Act), S.2007, 113th Cong. (2nd Sess. 2014).

54. Judit Takacs et al., *Validation of the Fitbit One Activity Monitor Device During Treadmill Walking*, 17 JOURNAL OF SCI. & MED. IN SPORT 496-500 (2014).

55. J. Adam Noah et al., *Comparison of Steps and Energy Expenditure Assessment in Adults of Fitbit Tracker and Ultra to the Actical and Indirect Calorimetry*, 37 JOURNAL OF MED. ENG'G & TECH. 456-62 (2013).

56. U.S. Food & Drug Admin., *General Wellness: Policy for Low Risk Devices Draft Guidance for Industry and Food and Drug Administration Staff*, U.S. FOOD AND DRUG ADMIN. (Jan. 20, 2015), http://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm429674.pdf.

the need for any regulation whatsoever by making it clear that they cannot be trusted for clinical use, for example, as described above.

This relatively simple method to clearly determine from the outset whether or not your mHealth app will be subject to FDA regulation (either you are Clinical or Recreational) should provide software with the freedom to innovate unimpededly without the overhanging fear of FDA regulations making their product unprofitable or unmarketable.

It is important to note that under this binary taxonomy, the important clinical innovations would not be lost. Eventually, the relatively mature innovation that has already passed through the general consumer recreational marketplace could be transferred to the clinical setting once the technology is proven in the recreational setting, and once the programmers and their backers better understand their product. And, hopefully at this juncture, the software producers will be better able to bring their more mature application through the FDA regulatory process.

Much of this may become quickly moot anyway. Once the novelty of having your smartphone conduct medical tests wears off, mHealth developers will likely quickly appreciate the liability concerns associated with the unknowable hardware and software with which is their application will interact, as described above. As such, future computational based developments will likely migrate to the cloud where variability associated with processing can be better limited and controlled. Further, whereas personal data collected on a smartphone, unless encrypted, represents a significant possibility of a breach of privacy,[57] the cloud could potentially provide a safe and secure environment for collected mHealth patient data.

Further, more astute mHealth app developers will likely pull away completely from smartphone-based analysis (since it is too risky given its unpredictable nature and inability to control all the moving parts) and market more profitable, controllable and reliable stand-alone devices. These stand-alone devices will likely be designed to not suffer from many of the general concerns related to using smartphones, including, network delays, limited bandwidth, confounding and conflicting software applications, viruses, malware, battery life, storage capacity and the like. For example, by 2014 there were nearly four million distinct malware software applications

57. Robert L. Garrie & Pamela E. Paustian, *mHealth Regulation, Legislation, and Cybersecurity*, in MHEALTH 45 (2014).

focused on mobile devices.[58] The growth of these devices will likely coincide with the growth of related telemedicine technologies.

Under the proposed binary taxonmy, in the end, it is likely that the only mHealth apps that will be regulated by the FDA will be those that in clinical settings perform "patient-specific analysis and providing patient specific diagnosis or treatment recommendations. Examples of mobile apps that perform sophisticated analysis or interpret data (electronically collected or manually entered) from another medical device include: apps that use patient-specific parameters and calculate dosage or create a dosage plan for radiation therapy; Computer Aided Detection software (CAD); image processing software; and radiation therapy treatment planning software."[59] These apps will run on stand-alone devices, designed specifically for the health market and in particular to avoid the uncertainties and liabilities associated with software apps running on old, hacked or otherwise non-optimal operating systems and technology platforms.

D. MMAs And Chronic Disease Patients

However, the underlying theories of this taxonomy fail when it comes to mHealth-related applications for the chronic disease demographic.[60] This is a relatively large percentage of the sick population: "In 2012, among civilian, noninstitutionalized US adults, approximately half (49.8%, 117 million) had at least 1 of 10 selected chronic conditions. More specifically, 24.3% had 1 chronic condition, 13.8% had 2 conditions, and 11.7% had 3 or more conditions."[61] Chronic diseases are the leading cause of morbidity and mortality in the United States.[62]

Part of treating chronic diseases is the promotion of healthy

---

58. Lianne Caetano, *Mobile Malware in 2014*, MCAFFEE BLOG CENTRAL (Mar 25, 2014), http://blogs.mcafee.com/consumer/mobile-malware-2014.

59. U.S. Food & Drug Admin., *supra* note 4.

60. *See, e.g.*, Christina Farr, *Former Google Executive's App Aims to Tackle Chronic Illness*, REUTERS (Oct. 28, 2014), *available at* http://www.reuters.com/article/2014/10/28/us-healthcare-tech-vida-idUSKBN0IH1SV20141028.

61. Brian W. Ward et al., *Multiple Chronic Conditions Among US Adults: A 2012 Update*, CENTERS FOR DISEASE CONTROL AND PREVENTION (April 17, 2014), http://www.cdc.gov/pcd/issues/2014/pdf/13_0389.pdf.

62. Ctrs. for Disease Control and Prevention, *Chronic Disease Overview*, CHRONIC DISEASE PREVENTION AND HEALTH PROMOTION (Feb. 23, 2016), *available at* http://www.cdc.gov/chronicdisease/overview/.

lifestyles and the self-management of the disease.[63] Self-management of chronic disease has been shown in studies to generally improve the health of patients and reduce the need for hospitalization, which itself exposes the patient to opportunistic infections.[64] Furthermore, some have estimated that mHealth technologies could offer 197 billion dollars in savings over the next two decades in treating chronic diseases.[65]

As such, this demographic may make up a large percentage of the mHealth market —in the United States, 86% of health care spending relates to the treatment of chronic disease[66] and this cannot be easily glossed over. It might include cancer, diabetes, heart disease, chronic obstructive pulmonary disease, HIV, and even obesity. These patients are the ones most likely to benefit from the constant monitoring and the constant connectivity of consumer electronics, allowing patients to self-manage their disease or provide for the ability to have timely interventions by a health professional when necessary,[67] provided that they actually use the applications. And, in clinical studies where chronic disease patients used mHealth technology, benefits were seen.[68]

With this demographic in mind, perhaps the above proposed taxonomy should include a hybrid group of applications that are both clinical and consumer directed, e.g., the passive collection of clinical or near-clinical grade data from consumer devices that can provide

---

63. Caroline Free, et al., *The Effectiveness of Mobile-Health Technology-Based Health Behaviour Change or Disease Management Interventions for Health Care Consumers: A Systematic Review*, 10 PLOS MEDICINE 1 (2013).

64. Kate R. Lorig, et al., *Evidence Suggesting That a Chronic Disease Self-Management Program Can Improve Health Status While Reducing Hospitalization: A Randomized Trial*, 37 MEDICAL CARE 5, 5-14 (1999).

65. Robert Litan, *Vital Signs via Broadband: Remote Monitoring Technologies Transmit Savings, Enhances Lives*, AT&T (Oct. 24, 2008), https://www.corp.att.com/healthcare/docs/litan.pdf.

66. Ctrs. for Disease Control and Prevention, *Chronic Disease Prevention and Health Promotion,* CTRS. FOR DISEASE CONTROL AND PREVENTION (Jan. 23, 2016) *available at* http://www.cdc.gov/chronicdisease/.

67. Tara McCurdie et al., *mHealth Consumer Apps: The Case for User-Centered Design*, 46 BIOMEDICAL INSTRUMENTATION & TECH. 49 (2012).

68. Charlene C. Quinn et al., *Welldoc™ Mobile Diabetes Management Randomized Controlled Trial: Change in Clinical and Behavioral Outcomes and Patient and Physician Satisfaction*, 10 DIABETES TECH. & THERAPEUTICS 160, 160-68 (2008); Charlene C. Quinn et al., *Cluster-Randomized Trial of a Mobile Phone Personalized Behavioral Intervention for Blood Glucose Control*, 34 DIABETES CARE 1934 (2011); *but c.f.* Bree Holtz & Carolyn Lauckner, *Diabetes Management Via Mobile Phones: A Systematic Review*, 18 TELEMEDICINE & E-HEALTH 175, 175-84 (2012) (noting that many of the studies lacked the requisite statistical rigor to come to medically relevant conclusions).

health care professionals with timely access to relevant data.

This hybrid group would include apps directed at consumers with chronic disease that require some form of constant monitoring. Alternatively, this group could also include apps directed to clinical study participants who need to track some or more of their vitals data off-site. This hybrid group might also interface with EHRs, albeit at home not at a health-care related institution.

But this hybrid group would also highlight many of the practical concerns raised above that cannot be simply solved by regulation or legislation. The need for some oversight is pressing and the drawn out iterative process of developing internal oversight controls, conformity assessment tools, certification and assessment schemes and general best practices (as suggested by the April 2014 FDASIA Health IT Report)[69] will fail to meet the urgent and exigent needs of the industry today. The same is true for IEEE and/or ISO standard proposals.[70]

Rather, a more technical solution may be necessary to overcome the issues raised and given the competing interests of public policy: dependable software with limited regulatory oversight.

E. Technological Soultions To Policy Concerns With Chronic Disease Oriented MMAS

To this end, a potential solution for both chronic disease apps as well as potentially even all MMAs currently regulated or otherwise would include a software or hardware interface to technologically deal with many of the concerns raised. This shared boundary between apps and anything else those apps communicate with would allow for the regulated and controlled exchange of information between any two different components of an mHealth environment. This could include an interface between the MMA and the underlying operating system and hardware or the MMA and an online component.

Developed under the auspices of a Federal agency, the middleware could be designed explicitly to deal with the many technical and regulatory concerns raised above. Like the Telecommunications Act of 1996, signed into law by President Bill

---

69. U.S. Food & Drug Admin., *FDASIA Health IT Report: Proposed Strategy and Recommendations for a Risk-Based Framework,* U.S. FOOD AND DRUG ADMIN. (Apr. 2014), http://www.healthit.gov/sites/default/files/fdasiahealthitreport_final.pdf.

70. *E.g.*, *ISO/IEEE 11073-10418:2014 Health Informatics—Personal Health Device Communication—Part 10418: Device Specialization—International Normalized Ratio (INR) Monitor,* INT'L ORG. FOR STANDARDIZATION (Mar. 1, 2014), *available at* http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=61897.

Clinton, that mandated that a specific technology (colloquially known as a V-chip) be introduced into every new television,[71] smartphones could also be required to include this middleware in all new phones and/or software updates.

The middleware could employ one or more open APIs (Application Programming Interface) such that any app developer could easily write their code to gather and/or distribute sensor data through the software interface.[72] This middleware could also create and enforce a single unified standard of sensor data such that independent of the hardware or the software (e.g., the smartphone and its operating system). Further, the middleware would also enforce a standardization of values resulting from sensors that allow for consistent readings independent of device hardware and software — for example, all values could be required to be presented using the metric system. Importantly, this standardization would allow for portability across hardware and software platforms and between other mHealth apps, something that seems to be widely lacking for most mHealth apps.[73]

This middleware could also enforce a standardization of medical information formats, limiting the usability of data that is not provided to the middleware from an mHealth app in standard format. This forced standardization would further promote good, reasonable and accurate use of collected health-related data. This standardization via the middleware could piggyback on current efforts to enforce standards in health care. For example, EHR standards could be imported and required for use in mHealth apps.[74,75]

In summary, the middleware proposed herein would be a standardized, calibrated, uniform platform to allow a standardized

---

71. Telecommunications Act of 1996, Title V – Obscenity And Violence, Pub. L. No. 104-104, 110 Stat. 56 (1996).

72. See, e.g., OPEN API INITIATIVE, openapis.org (last visited Aug. 10, 2015) (Describing how APIs form the connection between apps and third parties, and elaborating on how vendor neutral and open APIs can increase connectivity between apps and third party apps and/or data sources.)

73. Shoko Miyagawa et al., *Data Portability in Mhealth—Can We Retain Our Life Log When Changing Apps, Devices, or Mobile Platforms?*, 143rd APHA Annual Meeting and Exposition, APHA (Oct. 31-Nov. 4, 2015).

74. Marco Eichelberg et al., *Electronic Health Record Standards – A Brief Overview*, PROCEEDINGS OF THE 4TH IEEE INTERNATIONAL CONFERENCE ON INFORMATION AND COMMUNICATIONS TECHNOLOGY (2006).

75. A. Begoyan, *An Overview of Interoperability Standards for Electronic Health Records*, PENNSYLVANIA STATE UNIVERSITY (2007), http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.131.4421&rep=rep1&type=pdf.

communication between onboard and linked sensors and the individual mHealth applications. It is important that this middleware appear frictionless to the user and the developers, otherwise they will become a burden that users will attempt to work-around.

The middleware need not be specific to consumer based mHealth apps, and in fact, may be very useful in clinical apps as well. The middleware could be backwards compatible to legacy devices and constant updates would allow it to avoid becoming obsolete.[76]

To this end, the software might employ an onsite- or cloud based up-to-date database of hardware and software such that the necessary error corrections and fudge factors could be applied to varied sensor readings such that after these algorithms would be applied, the distinctions between all the varied types of hardware the software would be irrelevant. All applications receiving data from this software would start at the same baseline.

This same software could also employ regular calibrations and system checks both periodically during runtime and perhaps always at boot-up to confirm that the hardware has not been damaged through regular wear and tear and that the system's software has not been compromised as a result of uploaded code, malicious or otherwise.

The software interface could also be written such that it would not allow mHealth apps to circumvent it and acquire data from the sensors directly and not through the regulatory approved interface. Users might be given the opportunity to opt out of this limitation provided that they provide informed consent through, for example, a clickwrap license.[77]

As an additional benefit, this same middleware could also regulate the outflow of information from the individual mHealth apps, requiring that, for example, all mHealth collected data be encrypted for privacy protection. This encrypted outflow would employ one or more known encryption methodologies, i.e., limited and controlled encryption. This limited and controlled encryption would help promote interoperability among different devices and systems and

---

76. Philip A. Berstein, *Middleware: a model for distributed system services,* 39.2 COMMUNICATIONS OF THE ACM 86 (1996), http://delivery.acm.org/10.1145/240000/230809/p86-bernstein.pdf?ip=129.210.115.240&id=230809&acc=ACTIVE%20SERVICE&key=80B0E63637265656%2EC2822F75119601FF%2E4D4702B0C3E38B35%2E4D4702B0C3E38B35&CFID=668242243&CFTOKEN=78929755&__acm__=1473981831_09dba1f1823bd284ac448a70487df11b (describing some of the benefits of middleware, particularly when there are many different platforms that need to interact).

77. Nathan J. Davis, *Presumed Assent: The Judicial Acceptance of Clickwrap*, 22 BERKELEY TECH. L.J. 577 (2007).

network infrastructures, and in cases of emergency or legal need, it would be clear to the necessary agencies how to decrypt the data. Moreover, rather than relying on varying levels of encryption for each different application, this middleware could provide up-to-date, top-of-the-line encryption.

Further, software that used the mHealth app that did not encrypt data, or prevented the middleware from encrypting the data, would not work unless the user clicked through a sensibly composed clickwrap license[78] that made it clear that the data could only be employed for recreational use. Similarly, a clickwrap license would be required to be signed off on prior to sharing collected data.

Having a software solution as a required interface would limit the necessary regulatory outlays of the regulating agency. Much of the necessary complexity described above would, rather than being spread across literally thousands of applications, would all reside in one software program. Whether the application is developed by the FDA, some other regulatory agency or commercial group is not relevant. It is sufficient only that it would require some regulatory oversight to confirm that it remains accurate and useful.

Pushing this idea further, one could imagine a protected marketplace, run perhaps by the FDA and/or relevant NGO or governmental organizations where applications designed for clinical home use by chronic disease patients could be distributed, akin to the Apple iTunes market place, and distinct from the more open Android marketplaces. Like other proprietary app marketplaces, apps within the marketplace would have to pass a minimal standard. Further doctors could be encouraged to professionally review mHealth apps in this chronic disease marketplace by giving them continuing medical education (CME) credit for time spent in evaluating software. Evaluations would not be anonymous to prevent laziness and slacking and doctors and medical professionals would be encouraged to provide useful feedback that could be viewed by patients within the marketplace.

Apple's "Health"[79] (formerly Healthkit) may be the closest approximation of this goal for their proprietary devices: "Heart rate, calories burned, blood sugar, cholesterol — your health and fitness apps are great at collecting all that data. The new Health app puts that

78. *Id.*

79. HEALTH: AN INNOVATIVE NEW WAY TO USE YOUR HEALTH AND FITNESS INFORMATION, http://www.apple.com/ios/whats-new/health/ (last visited Oct. 31, 2015).

data in one place, accessible with a tap, giving you a clear and current overview of your health. With HealthKit, developers can make their apps even more useful by allowing them to access your health data, too."[80]

F. Other mHealth Concerns

In addition to the regulation of health care applications, and all concomitant bureaucracy associated with regulation, there remain a number of generalized concerns associated with mHealth. These concerns are not limited to the clinical apps, but are also relevant, if not even more so, for the unregulated recreational non-clinical applications.

Thus, even though we have argued that mHealth applications need not necessitate FDA oversight, particularly when they are specifically aimed at consumers and marked as recreational, nevertheless the continued growth of the non-medical consumer mHealth market raises a number of real and relevant concerns that need to be addressed.

For instance, "*[c]linicians and patients are adopting mobile technologies faster than providers can protect security and privacy. It's time to play catch-up.*"[81] Additionally, "[d]ata security and patient privacy are top issues facing everyone in the mHealth landscape, with regulators assessing the need for more rules and oversight, lawmakers calling on vendors to tighten data sharing practices and physicians citing the two issues as reasons for not embracing mHealth technology. A recent study cites the healthcare sector as the most immature industry in terms of personal mobile device security, endpoint compliance discovery and remediation."[82]

These security concerns are nearly insurmountable within the current status quo of cell phone usage. "Mobile phones are one of the most insecure devices that were ever available, so they're very easy to trace; they're very easy to tap."[83] Thus, it should come at no surprise

80. *Id.*

81. Bari Faudree & Mark Ford, *Security and Privacy in Mobile Health*, WALL ST. J. (Aug. 6, 2013), *available at* http://deloitte.wsj.com/cio/2013/08/06/security-and-privacy-in-mobile-health/.

82. Judy Mottl, *mHealth Success Hinges on Security, Workflow Adaptability*, FIERCE MOBILE HEALTHCARE (October 4, 2014), *available at* http://www.fiercemobilehealthcare.com/story/mhealth-success-hinges-security-workflow-adaptability/2014-10-04.

83. Evgeny Morozov, *Evgeny Morozov Quotes*, BRAINY QUOTE (Sept. 10, 2015), *available at* http://www.brainyquote.com/citation/quotes/quotes/e/evgenymoro555021.html?ct=Evgeny+Morozov; GOODMAN, *supra* note 43. *But cf.* Tim Cook, *A Message to Our Customers*,

that smartphones are huge security risks for health-related data.

In general, privacy concerns typically go hand-in-hand with security concerns, e.g., that someone will gain access to their personal and/or medical data and use it for fraud and/or identity theft. The promise to protect (and thus regulate) "security" of medical devices, (and now apps under the MMA guidance) is even spelled specifically in the FDA mission statement.[84] Nevertheless, even in areas where FDA regulation has been longstanding, there remain huge gaps in the regulation of security protocols for software.[85]

Security breaches, which have doubled in past year with an estimated 60% of android phones infected by malicious code,[86] can lead to a loss of consumer trust. [87] Even when security holes are identified it can be difficult if not impossible to have all consumers patch their software.

This inability to currently properly accommodate all of the private data purportedly being generated by mHealth apps is a huge liability for health care professionals and serves as a disincentive to popularize potentially useful apps.

According to the National Committee on Vital and Health Statistics (NCVHS), "the statutory public advisory body to the Secretary of Health and Human Services on health information policy",[88] "Health information privacy is an individual's right to control the acquisition, uses, or disclosures of his or her identifiable health data. Confidentiality, which is closely related, refers to the obligations of those who receive information to respect the privacy interests of those to whom the data relate. Security is altogether different. It refers to physical, technological, or administrative safeguards or tools used to protect identifiable health data from unwarranted access or disclosure."[89]

APPLE (Feb. 16, 2016), *available at* http://www.apple.com/customer-letter/ (Apple's opposition to the FBI's request to make a new version of the iPhone operating system).

84. U.S. Food & Drug Admin., *What We Do*, U.S. FOOD & DRUG ADMIN. (Dec. 7, 2015), *available at* http://www.fda.gov/aboutfda/whatwedo/.

85. *See* Eric D. Perakslis, *Cybersecurity in Health Care*, 371 NEW ENG. J. MED. 395 (Jul. 31, 2014).

86. Smart Clinic, *Breaking Down the mHealth Security Landscape*, SMART CLINIC BLOG (Sept. 25, 2014), http://smartclinicapp.com/breaking-mhealth-security-landscape/.

87. *See* Faudree & Ford, *supra* note 81.

88. NATIONAL COMMITTEE ON VITAL AND HEALTH STATISTICS, http://ncvhs.us/ (last visited Oct. 31, 2015).

89. Simon P. Cohn, *Recommendations Regarding Privacy and Confidentiality in the Nationwide Health Information Network*, NATIONAL COMMITTEE ON VITAL AND HEALTH STATISTICS (June 22, 2006), *available at* http://www.ncvhs.hhs.gov/recommendations-reports-

It is thought that there is a growing threat of cyberattacks associated with medical devices putting personal and private health information at risk for being disclosed: in this area, the FDA, which generally includes adverse event reporting and post-approval reports in its regulation of medical devices, lacks forward-looking approach to protect and prevent mHealth data before the malicious events occur. (Cybersecurity is conspicuously lacking from the MMA guidance documents).[90]

The substantial amount of literature relating to the general issues of patient privacy is one of the most pressing concerns of mHealth. Private data in the mHealth context can be thought of as broader than in the standard healthcare context. This is simply due to the reality that a broader array of data can be, and is, collected by mHealth applications. This data includes daily fitness data, exercise related information, calorie intake data, even levels of social interaction, and the more standard health-related information including glucose levels, blood oxygenation levels, heart rate, breathing rates, among others. Moreover, storing this data digitally makes it more portable and as such more likely to move via malicious actors.

With data saved locally on the device there are a number of opportunities for the personal health-related data to be captured and collected. Most simplistically, phones can be misplaced or hacked, as can large data online repositories. In fact, all the major online repositories, i.e., cloud computing providers, have been hacked.[91]

This data is not only at risk for privacy breaches while it is being collected by your smartphone using remote sensors, but it is also at risk while it sits on the phone and while it is transit between other systems, for example, where data is transferred wirelessly from smartphones to third party devices or cloud resource.

Transit of health-related and other privacy data can be a necessity, particularly for apps that require remote monitoring by health-related professionals. Additionally, data tends to be in transit during coordinated sharing between health care professionals that share the patient, and with remote/cloud storage such as, for example in commercial/consumer Personal Health Record (PHR) systems like

---

presentations/june-22-2006-letter-to-the-secretary-recommendations-regarding-privacy-and-confidentiality-in-the-nationwide-health-information-network/.

90. *See* Katherine B. Wellington, *Cyberattacks on Medical Devices and Hospital Networks: Legal Gaps and Regulatory Solutions*, 30 SANTA CLARA COMPUTER & HIGH TECH. L.J. 139 (2014).

91. GOODMAN, *supra* note 43, at 117.

the now discontinued Google Health,[92] Microsoft's HealthVault,[93] or the Dossia consortium,[94] or in an institutional Electronic Health Record (EHR) System.

Data transfers between phones and other devices, including the cloud, can be tapped and health data can be extracted and collected for any number or reasons, including, for example, identity theft, unauthorized access to data, or unauthorized and damaging disclosure of otherwise private health data.[95,96]Transit of data also occurs via wireless technologies such as Bluetooth and/or WiFi from wireless sensor devices or networks, e.g., wireless medical sensor networks (WMSNs). Data is often stolen or sniffed in transit. In some instances, femtocells and other devices that act as wireless network extenders, have been set up for malicious and illegal purposes. These extenders can trick phones into thinking that they are legitimate waypoints within the cellular network, wherein in reality they are designed to illicitly capture data.[97]

In addition to the most obvious victim of leaked information, the consumer, leaked data is also embarrassing for the corporate and health-related bodies involved in the processing and transferring of private patient data. Moreover, the leaking, stealing or sniffing of data could also expose risk-averse application developers to fines and lawsuits, thereby chilling innovation.

Guidelines could attempt to enforce encryption protocols to protect data. However, in consumer-facing apps, this type of enforcement is not feasible. Solutions exist, but they require the unprecedented and unlikely cooperation of the multitudes of mHealth app developers and/or the consumers to be implemented.[98] It is

---

92. GOOGLE HEALTH, http://www.google.com/intl/en_us/health/about/ (last visited Oct. 31, 2015).

93. HEALTH VAULT, https://www.healthvault.com/il/en (last visited Oct. 31, 2015).

94. DOSSIA CONSORTIUM, http://dossia.org/ (last visited Oct. 31, 2015).

95. David Kotz, *A Threat Taxonomy for mHealth Privacy* (2011), http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=5716518.

96. Consumer Reports, *Your Secrets Aren't Safe: Data Thieves are After Your Most Private Info—When You Use Wi-Fi and Shop Online, and Even When You Store Files in the Cloud*, CONSUMER REPORTS (May 2014), *available at* http://www.consumerreports.org/cro/magazine/2014/07/your-secrets-aren-t-safe/index.htm.

97. Lauren Walker, *Fake Cell Towers Allow the NSA and Police to Keep Track of You*, NEWSWEEK (Sept. 5, 2014), *available at* http://www.newsweek.com/what-cell-ls-those-ominous-phony-towers-268589; Kim Zetter, *Hacker Spoofs Cell Phone Tower to Intercept Calls*, WIRED (July 31, 2010), *available at* http://www.wired.com/2010/07/intercepting-cell-phone-calls.

98. Bruno M. Silva et al., *A Data Encryption Solution for Mobile Health Apps in*

unlikely that even suggested guidelines will be headed; app developers uninterested in the cumbersome and user-unfriendly encryption are unlikely to impose encryption without consumer demand. Additionally, consumers are unlikely to demand encryption since both hardware level encryption and software level encryption can affect phone performance and impact battery life; Google recently disclosed that up to 95% of its unencrypted traffic comes from mobile devices.[99] Most consumers do not protect their mobile phones with any technological protections.[100, 101,102] Even consumers that encrypt data on their own devices are unlikely to be sufficiently technologically savvy to encrypt communications between their applications and third parties. Moreover, the government itself is against strong encryption for smartphone data.[103, 104]

Privacy concerns might also result in a chilling effect, not only in the development of the mHealth apps and technologies, but in the prescription of their use by doctors wary of the fines and headaches associated with even minor HIPAA infractions.[105,106] Under the HIPAA Privacy Rule, HIPAA oversight is limited to privacy breaches associated with Protected Health Information (PHI), which only relates to identifiable information on an individual's mental and/or physical health, and only when that information is held or transmitted

---

Cooperation Environments, 15 J. MED. INTERNET RES. (2013).

99. GOOGLE TRANSPARENCY REPORT, https://www.google.com/transparencyreport/https (last visited March 15, 2016).

100. Sophos, *67 Percent of Consumers Don't Have Password Protection on Their Mobile Phones*, SOPHOS PRESS RELEASES (Aug. 9, 2011), *available at* https://www.sophos.com/en-us/press-office/press-releases/2011/08/67-percent-of-consumers-do-not-have-password-protection-on-their-mobile-phones.aspx.

101. Herb Weisbaum, *Most Americans Don't Secure Their Smartphones*, CNBC (Apr. 26, 2014), *available at* http://www.cnbc.com/2014/04/26/most-americans-dont-secure-their-smartphones.html.

102. Donna Tapellini, *Smart Phone Thefts Rose to 3.1 Million in 2013: Industry Solution Falls Short, While Legislative Efforts to Curb Theft Continue*, CONSUMER REPORTS (May 28, 2014), *available at* http://www.consumerreports.org/cro/news/2014/04/smart-phone-thefts-rose-to-3-1-million-last-year/index.htm.

103. *FBI Director Lashes Out at Apple, Google for Encrypting Smartphones*, RUSSIA TODAY (Sept. 26, 2014), *available at* http://rt.com/usa/190980-comey-fbi-encryption-phones/.

104. Maggie Ybarra, *FBI Pushes to Weaken Cell Phone Security, Skirt Encryption*, THE WASH. TIMES (May 26, 2015), *available at* http://www.washingtontimes.com/news/2015/may/26/fbi-push-to-weaken-cell-phone-security-skirt-encry.

105. *See* Health Information Technology for Economic and Clinical Health (HITECH) Act, 42 U.S.C. § 1320d-5(a)(3) (2013) (describing the four-tier penalty system for HIPAA violations).

106. Pardeep Kumar & Hoon-Jae Lee, *Security Issues in Healthcare Applications Using Wireless Medical Sensor Networks: A Survey*, 12 SENSORS 55, 65-73 (2012).

by a covered entity. Security breaches of ePHI fall under the HIPAA security rule which sets out technical administrative and physical standards to protect electronic persona health information.[107] Under the HITECH Act,[108] breach notifications need to be provided in instances of security failures and fines were raised significantly. Again this is limited only to covered entities; as such HIPAA regulations do not cover consumer directed mHealth applications.

And while HIPAA is regulated by The U.S. Department of Health and Human Services (HHS), not the FDA,[109] perhaps future efforts can include cooperation between the FDA and HHS in battling cyber security threats in the mHealth environment, including putting together best practices. Until such time, consumers need to rely on state and in some instances, federal consumer protection laws such as those enforced by the FTC.[110]

In addition to privacy concerns, a particularly important issue associated with the consumer mHealth apps is the concern that users, lacking the proper context and technical and medical knowledge will misunderstand or misinterpret the results, data, or information provided by the mHealth applications.

In some examples, this might result in rash prophylactic decisions carried out without medical supervision. These worried well individuals,[111] (iPodchondriacs[112]) some even clinically hypochondriacs, might limit otherwise normal behaviors, or otherwise act in unnecessary ways thinking that they are sick. Not only are these people harming themselves, but they might also become a drain on the medical system and insurers, visiting doctors and/or emergency rooms for unnecessary checkups or procedures. Unfortunately, the worried well are a lucrative demographic for mHealth developers, not only will they likely purchase health-related smart phone applications,

---

107. Modifications to the HIPAA Privacy Rule, 67 Fed. Reg. 53,182 (Aug. 14, 2002) (codified as 45 C.F.R. §§ 160, 164). The HIPAA Privacy Rule took effect on April 14, 2004. *Id.* at 53, 183.

108. The Health Information Technology for Economic and Clinical Health Act (HITECH) was enacted under Title XIII of the American Recovery and Reinvestment Act of 2009, Pub. L. No. 111–5, 123 Stat. 115 (2009).

109. 45 C.F.R. § 160.103.

110. Helm & Georgatos, *supra* note 6, at 151-67.

111. Maxine Frith, *Are You One of the Rising Numbers of the 'Worried Well'?*, THE TELEGRAPH (July 20, 2014), *available at* http://www.telegraph.co.uk/health/dietandfitness/10977877/Are-you-one-of-the-rising-numbers-of-the-worried-well.html.

112. *M-Health: Health and Appiness*, THE ECONOMIST (Feb. 1, 2014), *available at* http://www.economist.com/news/business/21595461-those-pouring-money-health-related-mobile-gadgets-and-apps-believe-they-can-work.

but it is expected that they will also purchase related peripherals that interact or integrate with smartphones and their applications at additional costs. Some analysts actually specifically track this demographics' uptake of mHealth-related technology. According to Machina research, for example, the worried well currently account for "61.8m connected devices in 2014 globally, increasing to more than 477m in 2023."[113]

On the other side of the spectrum are the walking sick. This demographic include groups of individuals that might otherwise need medical care, but have been lulled into a false sense of medical security based on results from their inaccurate or improperly used mHealth apps. They too can be a drain on insurers and health care providers, ignoring symptoms based on a false sense of security until the problems become bigger, more costly and impossible to ignore.

II. DEVELOPING WORLD ACCESS TO HEALTH CARE

The pros and cons mentioned above relate primarily to the United States and other developed nations. However, in some areas of the world, particularly where access to healthcare is severely limited, and outbreaks of major diseases are somewhat common,[114] mHealth can be a societal boon, particularly with the burden of chronic diseases rising in middle and low income countries.[115] As such, there have been numerous calls to scale up mHealth technologies in these areas.[116]

While access to health care is limited, particularly in rural areas of the world and in Africa, access to mobile technology, which is more affordable than most other basic services in Africa, is on a continual climb. Africa's mobile subscriber growth is effectively the fastest in the world, with estimates of over a billion mobile phone subscribers by 2015 and mobile penetration of almost 95% of the

113. Andy Castonguay, *Consumerization of Connected Health Devices Sparks Innovation and Growing Investment*, M2M NOW (May 20, 2014), *available at* http://www.m2mnow.biz/2014/05/20/20697-consumerization-connected-health-devices-sparks-innovation-growing-investment/.

114. Lizabeth Paulat, *Mobile Health Apps to Become First Line of Defense in Outbreaks*, VOICE OF AMERICA (Nov. 4, 2014), *available at* http://www.voanews.com/content/mobile-health-apps-to-become-first-line-of-defense-in-africa-outbreaks/2507423.html.

115. Robert Beaglehole et al., *Alma-Ata: Rebirth and Revision 3-Improving the Prevention and Management of Chronic Disease in Low-Income and Middle-Income Countries: A Priority for Primary Health Care*, 372 LANCET 940, 940 (2008).

116. *See* Tomlinson, *supra* note 14.

population.[117]

Mobile technology may bring about significant improvements to a healthcare system that is "constrained by high population growth, high disease burden, inadequate workforce, widespread rural populations and limited financial resources? The answer is mobile."[118]

Mobile communications may bring a wealth of knowledge to Africa that possesses the potential to "reimagine healthcare across Africa."[119] "From combating malaria to detecting counterfeit drugs, the emergence of mobile health solutions is saving more lives than international aids."[120] In a 2013 report by PricewaterhouseCoopers, the initiatives in Africa could potentially save a million lives by 2017.[121]

The mobile penetration notwithstanding, in spite of extensive efforts,[122] Africa still has the lowest rate of mHealth app adoption in the world, and in general lower and middle income countries lag behind their more developed neighbors.[123] Perhaps the promotion of standardized app middleware, as described above would further the uptake of, in some instances, vital software and technologies.

However, like the concerns mentioned above, even developing nations need to be cognizant of the particular pitfalls of mHealth technology – particularly its limitations and unintended consequences of too much or unclear information and data.

These same set of concerns, including privacy, security, walking sick and worried well, exist not only in the area of mHealth, but also in more recent developments in social media, which similarly

---

117. Amr Shady, *Africa's Mobile Market: Untapped Potential for Global Investment*, CP-AFRICA (Dec. 8, 2014), *available at* http://www.cp-africa.com/2014/12/08/africas-mobile-market-untapped-potential-global-investment/.

118. Louise Bleach, *How Kenya's Mobile Apps Are Changing the Face of Africa*, THE HUFFINGTON POST: THE BLOG (July 11, 2014, 7:41 AM), http://www.huffingtonpost.com/fueled/how-kenyas-mobile-apps-ar_b_5577233.html.

119. Seth Berkley, *How Cell Phones Are Transforming Health Care in Africa*, MIT TECH. REV. (Sept. 12, 2013), *available at* http://www.technologyreview.com/view/519041/how-cell-phones-are-transforming-health-care-in-africa/.

120. OluwaBusayo Sotunde, *10 Apps That Are Reshaping Healthcare In Africa*, VENTURES AFRICA (Nov. 23, 2014), *available at* http://www.ventures-africa.com/2014/11/10-apps-that-are-reshaping-healthcare-in-africa/.

121. *Id.*

122. Jessica L. Watterson et al., *Using mHealth to Improve Usage of Antenatal Care, Postnatal Care, and Immunization: A Systematic Review of the Literature*, 15 BIOMED RES. INT'L (Jan. 22, 2015), http://www.hindawi.com/journals/bmri/2015/153402/

123. Darrell West, *How Mobile Devices Are Transforming Healthcare*, ISSUES IN TECH. INNOVATION (May 2012), *available at* http://www.brookings.edu/~/media/research/files/papers/2012/5/22%20mobile%20health%20west/22%20mobile%20health%20west.

promote the sharing of personal medical data.

And, just like chronic disease patients are most likely to be major beneficiaries in the growth of mHealth, and patient monitoring applications, particularly those in underserved markets and countries, so too, the growth of patient oriented social media sites are likely to particularly help and benefit the growing population of patients with chronic diseases and their friends, family, and loved ones.[124,125] Given all this African market is prime for the introduction of the middleware described herein to support the nascent but growing mHealth infrastructure. Efforts should be taken here before stakeholders become too entrenched in their own non-standardized and unencrypted systems.

III. PATIENT ORIENTED SOCIAL MEDIA SITES

Patient Oriented Social Media Sites (POSOMS) are social media networks, i.e., public and private compilations of interconnected webpages, where patients with similar diseases and/or conditions can network. This networking differs substantially from more mainstream sites like Facebook[126] and Ello[127] in that participants are not seeking out friends but rather useful and relevant information relating to their diseases.[128]

In this networking, patients (often banking on reciprocity from fellow patients[129] and related individuals) can use, for example, associated tools and forums to help and inform each other with regard to their disease condition. This help can include sharing physician suggestions and rankings, as well as empirical, experimental, experiential, and anecdotal data related to drugs, therapies, side effects, and their referent diseases in general. This sharing of information has been found to be helpful both for the receiving community and also the individual sharing the information.[130]

---

124. Hamid Pousti et al., *Exploring the Role of Social Media in Chronic Care Management: A Sociomaterial Approach*, 446 IFIP ADVANCES INFO. COMM. TECH. 163, 170-81 (2014).

125. Adam D. Farmer et al., *Social Networking Sites: A Novel Portal for Communication*, 85 POSTGRADUATE MED. J. 455, 456-58 (2009).

126. FACEBOOK, www.facebook.com (last visited Oct. 31, 2015).

127. ELLO, https://ello.co/ (last visited Oct. 31, 2015).

128. Nima Kordzadeh et al., *A Multilevel Investigation of Participation Within Virtual Health Communities*, 34 COMMC'NS OF THE ASS'N FOR INFO. SYSTEMS 493, 493, 505-06 (2014).

129. *Id.* at 495.

130. Jeana H. Frost & Michael P. Massagli, *Social Uses of Personal Health Information*

These sites, more so than standard social networking sites, also provide often much-need emotional support from empathetic individuals who appreciate the situation.[131] These sites also allow patients to collectively check up on and/or validate potentially useful or damaging claims and statements related to their disease management;[132] this collaborative filtering may help protect patients from all the disinformation online.[133]

In terms of patients managing their own diseases, many of these sites provide users with proprietary symptom management tools, medical management tools, databases of drugs and diagnostic-related tools, among others, each used by members of the sites to varying degrees.[134] In some instances, patients can even employ these tools in their everyday interactions with their health care providers.[135]

Moreover, studies suggest that whereas particularly younger kids and teenage patients are unlikely to communicate regarding their disease in standard social media forums like Facebook and Twitter,[136] they may be more likely to do so in these specialized forums. As such, these particular forums present a particularly important social media safe haven for these patients. This is also the case for severely ill patients who might not have any other regular interactions with peers.[137]

These sites include Patientslikeme.com,[138] CureTogether.com,[139] CarePages.com,[140] HealthUnlocked.com,[141] Smart Patients.com,[142]

Within PatientsLikeMe, an Online Patient Community: What Can Happen When Patients Have Access to One Another's Data, 10 J. MED. INTERNET RES. (Aug. 25, 2008); Paul Wicks et al., *Sharing Health Data for Better Outcomes on PatientsLikeMe*, 12 J. MED. INTERNET RES. (June 14, 2010).

131. Kordzadeh et al., *supra* note 128, at 505-07.

132. Jeremy A. Greene et al., *Online Social Networking by Patients with Diabetes: A Qualitative Evaluation of Communication With Facebook*, 26 J. OF GEN. INTERNAL MED. 287, 288 (2011).

133. Gunther Eysenbach, *Medicine 2.0: Social Networking, Collaboration, Participation, Apomediation, and Openness*, 10 J. MED. INTERNET RES. (Aug. 25, 2008).

134. Wicks et al., *supra* note 130.

135. *Id.*

136. Maja Van Der Velden & Khaled El Emam, *"Not All My Friends Need to Know": A Qualitative Study of Teenage Patients, Privacy, and Social Media*, 20 J. AM. MED. INFORMATICS ASS'N 16, 20 (2013).

137. *See* Kate Khair et al., *Social Networking For Adolescents With Severe Haemophilia*, 18 HAEMOPHILIA 290, 294 (2012).

138. PATIENTSLIKEME, http://www.patientslikeme.com/ (last visited Oct. 31, 2015).

139. CURETOGETHER, http://curetogether.com/ (last visited Oct. 31, 2015).

140. CAREPAGES, https://www.carepages.com/ (last visited Oct. 31, 2015).

141. HEALTHUNLOCKED, https://healthunlocked.com/ (last visited Oct. 31, 2015).

UPOPOLIS ("a private online social network available exclusively to pediatric patients in hospitals and care facilities")[143] and others,[144] although not all are as democratic or as friendly as they make themselves out to be. It is not clear how many of the contributing patients and relatives appreciate and understand this.[145]

Some, like HealthTap.com,[146] are more app than social media, but nevertheless provide many of the same services to patients. Others, like Ginger.io are narrowly presented as only for collecting patient crowdsourced data.[147] Still others, while providing many of the support services, are focused solely on collecting data, not for pharmaceutical and health-related studies, but for marketers to these patient communities.[148] And others like Treato.com, are not online communities in and of themselves, but rather, scrapers that search the Internet for related data and information.[149]

Overall the trend toward a growing number of patient oriented social media sites seems like a positive development for patients and their friends and families, who even in well-served markets might otherwise not have sufficient and/or necessary access to support groups and/or healthcare professionals on a regular basis. Even finding medical professionals specializing in a particular disease, an exercise that can sometimes be difficult, particularly for patients just recently informed of their condition, can be facilitated in these forums. Additionally POSOMS are important tools for patients to simply collect catalogue and disseminate information about their disease; oftentimes particularly rare diseases suffer from a lack of accessible information.[150] POSOMS can be the only lay source of reliable information.

Moreover, these sites have the potential to provide all patients

---

142. SMART PATIENTS, https://www.smartpatients.com/ (last visited Oct. 31, 2015).

143. UROPOLIS, https://www.upopolis.com/ (last visited Oct. 31, 2015).

144. *See, e.g.,* Grazia Orizio et al., *The World of e-Patients: A Content Analysis of Online Social Networks Focusing on Diseases*." 16 TELEMEDICINE & E-HEALTH 1060, 1062 (2010), for a relatively early and lengthy list.

145. *See* Deborah Lupton, *The Commodification of Patient Opinion: The Digital Patient Experience Economy in the Age of Big Data*, 36 SOC. HEALTH & ILLNESS 856, 866 (2014).

146. HEALTHTAP, https://www.healthtap.com/ (last visited Oct. 31, 2015).

147. GINGER.IO, https://ginger.io/ (last visited Oct. 31, 2015).

148. ALLIANCE HEALTH, https://www.alliancehealth.com/ (last visited Oct. 31, 2015).

149. TREATO, http://treato.com/ (last visited Oct. 31, 2015).

150. Kimberly K. Walker, *Rare Disease-Specific Social Media Sites: An Opportunity for Collaboration*, 6 J. COMMC'N IN HEALTHCARE 71 (2013).

with data to make better informed decisions about their health[151] and/or to share with similarly afflicted individuals other important and relevant information about care and disease management.[152, 153] And, in general, these more informed patients can be more responsible for their health and make more rational decisions.[154] This combined with perhaps the need for fewer in-person visits can relieve strain on a healthcare system.[155]

Additionally, social relationships, be they online or in person (although some have suggested that online networks may erode otherwise useful real-world networks[156]), have been shown to have positive effects on a patient's condition disease management[157] and disease outcome.[158,159] Conversely, the lack and/or loss of a social network have been known to be detrimental.[160, 161] These sites may also provide the necessary incentives to mitigate attrition from the self-monitoring apps described above.[162,163] Further these sites and

---

151. Mario Christodoulou, *Networking: The New Social Revolution in Health Care*, 12 THE LANCET ONCOLOGY, 125 (2011).

152. Wicks et al., *supra* note 130.

153. *See* Noriko Hara & Khe Foon Hew, *Knowledge-Sharing in an Online Community of Health-Care Professionals*, 20 INFO. TECH. & PEOPLE 235 (2007).

154. Konstantinos Bletsos et al., *Towards a Fourth Cosmology of Doctor-Patient Relationship: A Reflection on the Virtual Patient Community PatientsLikeMe*, 11 TRIPLEC: COMMC'N, CAPITALISM & CRITIQUE 136 (2013).

155. Wicks et al., *supra* note 130.

156. R. Mackey, *Is Social Networking Killing You?*, THE LEDE: THE N.Y. TIMES NEWS BLOG (Feb. 24, 2009, 4:16 PM), http://thelede.blogs.nytimes.com/2009/02/24/is-social-networking-killing-you/?_r=0. *But see* Robert Kraut et al., *Internet Paradox Revisited*, 58 J. SOC. ISSUES 49 (2002).

157. *See* Jingquan Li, *Improving Chronic Disease Self-Management through Social Networks*, 16 POPULATION HEALTH MGMT. 285, 285-87 (2013).

158. Nicole B. Ellison et al., *The Benefits of Facebook "Friends:" Social Capital and College Students' Use of Online Social Network Sites*, 12 J. COMPUTER MEDIATED COMMC'N 1143 (2007).

159. *See* Eunkyung Kim et al., *The Process and Effect of Supportive Message Expression and Reception in Online Breast Cancer Support Groups*, 21 PSYCHO-ONCOLOGY 531 (2012).

160. *See* Nicholas A. Christakis & Paul D. Allison, *Mortality after the Hospitalization of a Spouse*, 354 NEW ENG. J. MED. 719 (2006).

161. *See* Julie Knoll Rajaratnam et al., *The Effect of Social Isolation on Depressive Symptoms Varies by Neighborhood Characteristics: A Study of an Urban Sample of Women With Pre-School Aged Children*, 6 INT'L J. OF MENTAL HEALTH & ADDICTION 464 (2008); Jeffrey V. Johnson et al., *Combined Effects of Job Strain and Social Isolation on Cardiovascular Disease Morbidity and Mortality in a Random Sample of the Swedish Male Working Population*, 15 SCANDINAVIAN J. WORK, ENV'T & HEALTH 271 (1989).

162. Gunther Eysenbach, *eHealth (Web-Based Behavior Change Programs) in the Toronto Star*, GUNTHER EYSENBACH'S RANDOM RESEARCH RANTS (Nov. 17, 2008), http://gunther-eysenbach.blogspot.com/2008/11/ehealth-web-based-behavior-change.html.

associated social networks allow patients to develop positive self-images in relation to their disease.[164]

Patient oriented social media sites can also be particularly powerful for the underserved. In many instances socially and/or culturally disadvantaged patients may have trouble following and interacting with medical professionals in an office setting, but may find it easier to interact online in a more relaxed setting with computing tools that provide quick translation or definitions of complicated jargon.

A. Concerns With Patient Oriented Social Media Sites

While POSOMS have been around for at least a decade, there remain a number of interesting heretofore unanswered research questions, including: (1) how do these networks affect health-related decisions; (2) to what extent do different individuals on these networks influence patients, individually and collectively; (3) what is the role of a physician and other healthcare workers vis-à-vis these sites; and (4) how does activity on these sites affect patient-health-worker relationships offsite?[165] Additionally, are patients being exploited by these sites or others trolling the sites?[166]

1. Patient Privacy

A particularly pertinent issue relates to patient privacy on these websites.[167] Patients on these sites are encouraged to share their data.[168, 169] While privacy is a general concern online, and particularly in social media, where simply tracking someone's seemingly benign "likes" and/or status updates can identify and characterize her,[170]

---

163. *But see* Cory A. Heidelberger et al., *Online Health Social Networks and Patient Health Decision Behavior: A Research Agenda*, IEEE COMPUTER SOCIETY (2011), https://www.computer.org/csdl/proceedings/hicss/2011/4282/00/07-05-09.pdf.

164. *See* Greene et al., *supra* note 132.

165. Heidelberger et al., *supra* note 163.

166. Natasha Singer, *When Patients Meet Online, Are There Side Effects?*, N.Y. TIMES (May 29, 2010), *available at* http://www.nytimes.com/2010/05/30/business/30stream.html?_r=0.

167. Jingquan Li, *Privacy Policies for Health Social Networking Sites*, 20 J. AM. MED. INFORMATICS ASS'N 704 (2013).

168. Deborah Lupton, *The Commodification of Patient Opinion: The Digital Patient Experience Economy in the Age of Big Data*, 36 SOCIOLOGY HEALTH & ILLNESS 856 (2014).

169. Katherine C. Chretien & Terry Kind, *Social Media and Clinical Care Ethical, Professional, and Social Implications*, 127 CIRCULATION 1413 (2013).

170. Golnoosh Farnadi et al., *Recognising Personality Traits Using Facebook Status Updates*, *in* Proceedings of the Workshop on Computational Personality Recognition

these concerns are exacerbated in POSOMS where a patient's guard may be down in a seemingly safe environment[171] and where they might tend to share more personal and health-related information than they might otherwise on non-health-related websites. It takes very little information to deanonymize someone's online profile, as was recently shown when Netflix's anonymous database of movie preferences was deanonymized when the provided anonymous information was cross-referenced with the IMDB database.[172] Similarly, one's anonymous POSOM profile may be deanonoymized by comparing it to, say, a database of Facebook profiles.

There is also the possibility that a patient's disclosure on these sites, or even simply her membership on the site, could affect her or her close families' ability to obtain health and/or life insurance a job and a relationship.[173,174] It remains unclear as to how the Genetic Information Nondiscrimination Act (GINA) would prevent employers and health care providers from using information freely shared on these sites – even anonymous sharing that might be relatively easily deanonymized.[175] SNOPA, the Social Networking Online Protection Act, was an effort to plug some of these gaps. It has so far been unable to become law.[176]

2. Defamation

Many patients feel that these sites are safe havens for communicating otherwise sensitive and stigmatizing information.[177] This feeling of a safe haven combined with the desire to share

(WCPR13) at the 7th International AAAI Conference on Weblogs and Social Media (2013); Michal Kosinski et al., *Private Traits and Attributes are Predictable From Digital Records of Human Behavior*, 110 PROC. NAT'L ACAD. SCI. 5802 (2013); Yoram Bachrach et al., *Personality and Patterns of Facebook Usage*, *in* Proceedings of the 3rd Annual ACM Web Science Conference (2012); Dejan Markovikj et al., *Mining Facebook Data for Predictive Personality Modeling*, *in* Proceedings of the 7th International AAAI Conference on Weblogs and Social Media (2013).

171. *See* Li, *supra* note 157.

172. Arvind Narayanan & Vitaly Shmatikov, *Robust De-Anonymization of Large Sparse Datasets*, *in* 2008 IEEE Symposium on Security and Privacy (2008).

173. *See* Van Der Velden & El Emam, *supra* note 136.

174. Daniel J. Solove, *The End of Privacy?*, 299 SCI. AM. 100 (2008).

175. Sandra Soo-Jin Lee & Emily Borgelt, *Protecting Posted Genes: Social Networking and the Limits of GINA*, 14 AM. J. BIOETHICS 32 (2014).

176. Social Networking Online Protection Act, H.R. 5050, 112th Cong. (2012); Social Networking Online Protection Act, H.R. 537, 113th Cong. (2013). These acts died in committee, *see, e.g.*, https://www.govtrack.us/congress/bills/112/hr5050.

177. Jacqueline L. Bender et al., *Seeking Support on Facebook: A Content Analysis of Breast Cancer Groups*, 13 J. MED. INTERNET RES., Jan.–Mar. 2011.

relevant information online described above can also lead to actionable defamation of doctors and health care workers.[178] As per the Restatement (Second) of Torts (1977), "[t]o create liability for defamation there must be: (a) a false and defamatory statement concerning another; (b) an unprivileged publication to a third party; (c) fault amounting at least to negligence on the part of the publisher [with respect to the act of publication]; and (d) either actionability of the statement irrespective of special harm or the existence of special harm caused by the publication."[179]

Further, "[a] communication is defamatory if it tends so to harm the reputation of another as to lower him in the estimation of the community or to deter third persons from associating or dealing with him."[180] Most social media sites, including POSOMS, can be described as public forums, and like their offline counterparts, members have to be cognizant of the limitations of their speech.

Members on POSOMS face even greater dangers than standard run-of-the-mill social media sites which themselves suffer from the lack of fail safes (e.g. time and editors) that typically protect individuals in offline public forums from defaming and/or libeling individuals.[181] Moreover, patients may feel that the information that they are presenting regarding a healthcare worker will help other patients and as such might be more likely to post something defamatory as a result than on other social media sites. Note that while defamation can be found by a court even when the defamatory statement is phrased as an option, many states provide laws and anti-SLAPP statutes that protect some forms of speech when the speech was without malice and when it was believed to be true.[182]

Even pharmaceutical companies can sue for libel and/or defamation for online defamatory and/or libelous comments, a likely occurrence on these sites where patients may be advising other

178. Brian Chou and Walt Mayo, *'I was Dissed on Angie's List,'* REVIEW OF OPTOMETRY (April 15, 2009), *available at* https://www.reviewofoptometry.com/article/i-was-dissed-on-angies-list; Nicolas P. Terry, *Fear of Facebook: Private Ordering of Social Media Incurred by Healthcare Providers,* 90 NEB. L. REV. 703 (2012).

179. RESTATEMENT (SECOND) OF TORTS § 558 (1977).

180. *Id.* § 559.

181. Ian Burrell, *Libel Cases Prompted by Social Media Posts Rise 300% in a Year*, INDEP. (Oct. 19, 2014), *available at* http://www.independent.co.uk/news/uk/home-news/libel-cases-prompted-by-social-media-posts-rise-300-in-a-year-9805004.html.

182. Elec. Frontier Found., *Online Defamation Law*, ELECTRONIC FRONTIER FOUNDOUNDATION *available at,* https://www.eff.org/issues/bloggers/legal/liability/defamation.

patients. [183]However, at least in the United States, under the Communications Decency Act of 1996, the social media network itself is likely immune from defamations made by members or third parties,[184] leaving behind few deep pockets to sue.[185]

In some instances where it might be obvious that the putatively defamatory comment is an opinion, the individual publishing the opinion may also not be liable.[186] Thus, when "a "reasonable reader would not view the blanket, unexplained statements at issue as "facts," [rather...] subjective speculation' or "merely rhetorical hyperbole," there may be no liability unless the plaintiff proves "that a statement is factually based and thus capable of a defamatory meaning."[187]

3. Abuse Of Trust

Patient-oriented social media sites may also present opportunities for others to prey on patients and their families, for example, by individuals misrepresenting their medical credentials, or lack thereof.[188] This can also include doctors or other healthcare workers who are looking for individuals to sign up for clinical studies. Rather than going through standard channels, doctors can come to these social media sites to find a consolidated and interested population with disclosed medical histories and conditions so that they can find the best-suited individuals for their trials. A number of clinical trials have already been staffed through contacting patients via POSOMS.[189] And while the FDA has specific rules for trial

183. Nanoviricides, Inc. v. Seeking Alpha, Inc., No. 151908/2014, 2014 WL 2930753 (N.Y. Sup. June 26, 2014); *Biomatrix* Corp., *et al*. *v*. *Costanzo*, *et al*., *Docket No*. *BER-L-670-00* (Superior Court of New Jersey, Bergen County); Eric Niiler, *Internet Chat Damages Biotechnology Stocks*, NATURE BIOTECHNOLOGY (2000), *available at* http://www.nature.com/nbt/journal/v18/n10/full/nbt1000_1030b.html; Aaron Elstein, *Judge Rules Online Postings About Biomatrix Were Libel*, WALL ST. J. (Aug. 3, 2000), *available at* http://www.wsj.com/articles/SB965239740373615064.

184. *E.g.*, Zeran v. America Online, Inc., 129 F.3d 327, 330 (4th Cir. 1997)*, cert. denied*, 524 U.S. 937 (1998) (ruling that Section 230 of the Communications Decency Act "creates a federal immunity to any cause of action that would make service providers liable for information originating with a third-party user of the service."); *see also* Barrett v. Rosenthal, 40 Cal. 4th 33 (2006).

185. 47 U.S.C. § 230(c)(1) (2012) ("No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.").

186. Doe v. Cahill, 884 A.2d 451, 466 (Del. 2005).

187. *Id.* at 467-68 n.78.

188. Chretien & Kind, *supra* note 169.

189. Melanie Swan, *Emerging Patient-Driven Health Care Models: An Examination of*

recruitment, they are not geared to online recruitment,[190] and may or may not clearly be applied.[191]

Even worse, snake-oil salesmen might present themselves as legitimate pharmaceutical representatives or medical professionals to sell useless or even harmful concoctions to the unassuming public within what seems to them, to be a protected environment.[192]

In general, doctors and others trolling for bodies for their trials should not do so anonymously, particularly when their perceived lack of duty to someone else's patient might result in them choosing individuals who are best for the trial, although not necessarily pointing out trials that are best for the individuals. Further, patients, who might otherwise not sign up for clinical trials unless they were presented to them by their trusted physician, may sign up for trials that might not be in their best interests when approached online. In some instances, a patient may sign up for what they perceive to be a legitimate IRB approved trial, when in reality it is an ad hoc trial by an unregulated body.

Additionally, concerns should be raised given that pharmaceutical representatives or their paid agents can promote, under the anonymity provided by the internet, their product, promote off label use, disparage competing products, and use other marketing tactics without disclosing their conflicts of interest. Even overtly, patients may be influenced by directed marketing to choose one drug over another. Pharmaceutical companies have made substantial efforts in these areas, including, for example, conversational marketing (i.e., to make online friends and then turn those friends into customers) and efforts to create online threads lead by peer influencers.[193] In some instances, patients are not even interacting with real individuals but

---

Health Social Networks, Consumer Personalized Medicine and Quantified Self-Tracking, 6 INT'L J. ENVTL RES. & PUBLIC HEALTH 492 (2009).

190. Jim Gearheart, *Clinical Trial Recruitment Using Social Media is Growing*, 5 QUORUM REVIEW IRB (Mar. 5, 2015), *available at* http://www.quorumreview.com/blog/2015/03/05/clinical-trial-recruitment-social-media-growing/.

191. Kristen Snipes, *Rho Regulatory Considerations for Using Social and Digital Media in Clinical Trial Patient Recruitment*, CLINICAL INFORMATICS NEWS (May 26, 2015), *available at* http://www.clinicalinformaticsnews.com/2015/3/26/regulatory-considerations-using-social-digital-media-clinical-trial-patient-recruitment.html.

192. Bradford W. Hesse et al., *Social Participation in Health 2.0*, 43 COMPUTER 45 (2010).

193. Manon Niquette, *The Exploitation of "Sicko-Chatting" by the Pharmaceutical Industry: A Strategy for the Normalization of Drug Use*, SCIENTIFIC PUBLICATIONS OF THE HUMANITIES AND SOCIAL SCIENCES UNIVERSITY OF LILLE (2013), *available at* http://hal.univ-lille3.fr/hal-00835818v2.

rather artificial intelligence software aimed at creating new customers.[194] The extent of pharmaceutical representation on these sites is unknown, as is the extent that pharmaceuticals promote openly, or using sock puppets,[195] their products.[196]

Finally, the aggregation of lay-minded patients on these website can influence policy, regulation and crowdsourced funded research both positively, and potentially negatively, if the lay-minded patients are taken advantage of; each privately run POSOM potentially is its own institution with its "own leadership, goals and agenda."[197]

a. Regulation Of Patient Oriented Social Media Sites

All these concerns notwithstanding, the FDA has been loath to substantively regulate social media in general[198] and specifically as it relates to pharmaceutical advertising.[199] Social media is actually already subject to some diverse sets of regulation. For example, on standard social media sites, many non-pharmaceutical ads are regulated via the FTC, financial communications with customers via social media is regulated by the Financial Industry Regulatory Authority, and the National Labor Relations Board provides regulation regarding employer restrictions on access to social media.[200]

However, like their efforts to regulate mobile medical applications as devices, the FDA should similarly regulate broader aspects of social media, particularly when those aspects of social media as designed specifically for use in healthcare and health delivery. While the FDA held public hearings in 2009 on issues

194. A similar example can be found from disclosures from the Ashley Madison website. *See, e.g.,* Annalee Newitz, *How Ashley Madison Hid Its Fembot Con From Users and Investigators,* GIZMODO (Sept. 8, 2015), *available at* http://gizmodo.com/how-ashley-madison-hid-its-fembot-con-from-users-and-in-1728410265.

195. Chelsea Peters, *Whole Foods, Unwholesome Practices: Will Sock Puppeteers Be Held Accountable for Pseudonymous Web Postings*, 5 SHIDLER J.L. COM. & TECH. 4, 5 (2008).

196. Greene et al., *supra* note 132.

197. Swan, *supra* note 189.

198. Venkatesh Shankar & Jiaoyang (Krista) Li, *Leveraging Social Media in the Pharmaceutical Industry*, in INNOVATION AND MARKETING IN THE PHARMACEUTICAL INDUSTRY 477 (Min Ding et al. eds., 2014).

199. U.S. Food and Drug Admin., *For Industry: Using Social Media*, ABOUT FDA (Oct. 29, 2014), *available at* http://www.fda.gov/AboutFDA/CentersOffices/OfficeofMedicalProductsandTobacco/CDER/ucm397791.htm.

200. Jon Poracro, *Social Media Laws and Regulations You Should Know*, METIA (Aug. 26, 2011), *available at* http://www.metia.com/seattle/john-porcaro/2011/08/social-media-laws-and-regulations-you-should-know/.

relating to promotional speech through social media,[201] it has only very recently released very limited guidance relating to discussing pharmaceuticals on social media sites. In the interim, while the FDA's Office of Prescription Drug Promotion, formerly known as the Division of Drug Marketing, Advertising, and Communications, whose goal is to:

> To protect the public health by assuring prescription drug information is truthful, balanced and accurately communicated. This is accomplished through a comprehensive surveillance, enforcement and education program, and by fostering better communication of labeling and promotional information to both healthcare professionals and consumers.[202]

In fact, the FDA has sent out only one regulatory action letter to a pharmaceutical company where social media was the basis for the offensive action in the years between 2008 and 2013.[203] The only real substantive guidance provided by the FDA in relation to social media sites relates to correcting false information online – in short there is no duty to correct online misinformation and traditionally, pharmaceuticals have steered clear of correcting misinformation for fear of backlash from the FDA. [204]The new guidance however also allows companies the right to correct misinformation, provided that the correction is "relevant and responsive," "limited and tailored," "non-promotional," and "accurate."[205] With this burden, it is unclear how many pharmaceutical companies will take the opportunity to

---

201. U.S. Food and Drug Admin., *Public Hearing on Promotion of FDA-Regulated Medical Products Using the Internet and Social Media Tools,* ABOUT FDA (Nov. 27, 2015), *available at* http://www.fda.gov/AboutFDA/CentersOffices/OfficeofMedicalProductsandTobacco/CDER/ucm184250.htm.

202. U.S. Food and Drug Admin., *The Office of Prescription Drug Promotion*, ABOUT FDA (Oct. 23, 2015) *available at* http://www.fda.gov/AboutFDA/CentersOffices/OfficeofMedicalProductsandTobacco/CDER/ucm090142.htm.

203. Mark S. Senak, *FDA Communications Oversight in a Digital Era 2008-2013*, EYEONFDA (Apr. 2013), *available at* http://www.eyeonfda.com/wp-content/uploads/2013/03/FDA-Communications-Oversight-in-a-Digital-Era1.

204. *See, e.g.,* Policy and Medicine, *FDA Social Media Guidance: Correcting Independent Third-Party Misinformation About Prescription Drugs and Medical Devices*, POLICY AND MEDICINE (June 18, 2014), *available at* http://www.policymed.com/2014/06/fda-social-media-guidance-correcting-independent-third-party-misinformation-about-prescription-drugs-and-medical-devices.html ("Previously, companies have struggled with the best way to approach this type of online misinformation. FDA's Guidance provides clarity").

205. U.S. Food & Drug Admin., *Guidance for Industry: Internet/Social Media Platforms: Correcting Independent Third-Party Misinformation About Prescription Drugs and Medical Devices,* U.S. FOOD AND DRUG ADMIN. (June 2014), http://www.fda.gov/downloads/drugs/guidancecomplianceregulatoryinformation/guidances/ucm401079.pdf.

correct misinformation when they are legally safer to not say anything. Note: there is also guidance for pharmaceuticals with relation to microblogging.[206]

Other governmental agencies are also interested in some aspects of POSOMS, including for example the FTC's interest in the patient privacy aspects related to patient data that is collected and catalogued on many of these sites.[207]

The lack of FDA and other governmental oversight of POSOMS will become increasingly problematic as both industry[208] and regulators themselves[209] look to POSOMS as sources of crowdsourced, user generated data for use in research and development of medicine and other health-related technologies.

b. Patient Oriented Social Media Sites And Data Creation And Collection

Obviously, POSOMS do not only help patients and their families, other stakeholders benefit substantially from the data that can be mined from these websites. Patients on these sites should be wary: "When something online is free, you're not the customer, you're the product."[210] Patientslikeme.com, and presumably other similar social media websites make money by selling personal and potentially private information.[211,212] Even when they are not outright

---

206. *Id.*

207. Fed. Trade Comm'n, *FTC Announces Agenda, Panelists for Upcoming Seminar on Privacy Implications of Consumer Generated and Controlled Health Data,* FED. TRADE COMM'N PRESS RELEASES (May 1, 2014), *available at* http://www.ftc.gov/news-events/press-releases/2014/05/ftc-announces-agenda-panelists-upcoming-seminar-privacy.

208. Jennifer Levin, *AstraZeneca and PatientsLikeMe Announce Global Research Collaboration*, FIERCEBIOTECH (April 14, 2015), *available at* http://www.fiercebiotech.com/press-releases/astrazeneca-and-patientslikeme-announce-global-research-collaboration.

209. Thomas Sullivan, *PatientsLikeMe Teams With FDA To Explore Patient-Reported Adverse Events*, POLICY AND MEDICINE (July 9, 2015), *available at* http://www.policymed.com/2015/07/patientslikeme-teams-with-fda-to-explore-patient-reported-adverse-events.html.

210. Jonathan Zittrain, *The Future of the Internet and How to Stop It*, HARVARD LAW BLOGS (Mar. 21, 2012), http://blogs.law.harvard.edu/futureoftheinternet/2012/03/21/meme-patrol-when-something-online-is-free-youre-not-the-customer-youre-the-product/.

211. PatientsLikeMe, *Does PatientsLikeMe Sell My Information?*, PATIENTSLIKEME (2014), *available at* https://support.patientslikeme.com/hc/en-us/articles/201245770-Does-PatientsLikeMe-sell-my-information- ("The data and text you enter in and around the shared parts of the site (e.g., on your profile, in the forum, symptom or treatment reports) may be shared or sold in aggregate to partners.").

212. Jim Edwards, *PatientsLikeMe is More Villain than Victim in Patient Data "Scrapping" Scandal*, CBS MONEYWATCH (Oct. 19, 2010), *available at* http://www.cbsnews.com/news/patientslikeme-is-more-villain-than-victim-in-patient-data-scraping-scandal/ ("Here's what type of data PatientsLikeMe scrapes from its own site for its clients:

selling data, other companies may be scraping (i.e., "collecting online data from social media and other Web sites in the form of unstructured text . . . also known as site scraping, web harvesting and web data extraction")[213] personal data from these sites.[214]

POSOMs are incentivized to get as many patients as possible to sign up and eventually even disclose their health-related data, as they, their corporate consumers and the patients themselves can benefit from the network effects resulting from greater participants.[215]

PatientsLikeMe, founded in 2004, is one of the more popular patient oriented social media sites. With more than a quarter of a million members and 2000 health conditions, the site was noted in 2007 as a company that will change the world.[216] The site is configured to allow patients with similar diseases connect with their peers to share information. And like many of the mHealth apps described above, PatientsLikeMe.com and other similar sites empower patients to learn more and do more about their health condition.

This patient empowerment is part of a general trend that includes crowdsourcing, citizen science.[217] uBiome (a citizen science startup)[218] and other forms of participant led research — sometimes known as prosumption (the simultaneous production and consumption of information)[219]— can empower the patient, subject, or non-health

---

Condition/disease information, including diagnosis date, first symptom information, and family history; Treatment regimens, including treatment start dates, stop dates, dosages, and side effects; Symptoms experienced, including severity and duration; Laboratory results (e.g. CD-4 count, Viral Load); Biographical information, including photo, bio, gender, age, location (city, state & country), and general notes; Genetic information, including information on individual genes and/or entire genetic scans").

213. Bogdan Batrinca & Philip C. Treleaven, *Social Media Analytics: A Survey of Techniques, Tools and Platforms*, 30 AI & SOC'Y 89 (2015).

214. Julia Angwin & Steve Stecklow, *'Scrapers' Dig Deep for Data on Web*, WALL ST. J. (Oct. 12, 2010), *available at* http://www.wsj.com/news/articles/SB10001424052748703358504575544381288117888?mod=WSJ_0_0_WP_2715_RIGHTTopCarousel_1&mg=reno64wsj&url=http%3A//online.wsj.com/article/SB10001424052748703358504575544381288117888.html%3Fmod%3DWSJ_0_0_WP_2715_RIGHTTopCarousel_1.

215. Frost & Massagli, *supra* note 130.

216. Erick Schonfeld & Chris Morrison, *The Next Disruptors*, CNN MONEY (Aug. 22, 2007), *available at* http://money.cnn.com/magazines/business2/business2_archive/2007/09/01/100169862/index.htm.

217. Rick Bonney et al., *Citizen Science: A Developing Tool for Expanding Science Knowledge and Scientific Literacy*, 59 BIOSCIENCE 977 (2009).

218. UBIOME, http://ubiome.com/ (last visited Nov. 1, 2015).

219. David Beer & Roger Burrows, *Consumption, Prosumption and Participatory Web Cultures: An Introduction*, 10 J. CONSUMER CULTURE 3 (2010); George Ritzer & Nathan

practitioner stakeholder to partially direct, control or simply have a greater degree of input in the analysis than they otherwise mite via the classical investigator led research (ILR) paradigm.[220]

Some have argued that these non-commercial, disease-oriented, and patient-controlled studies provide a greater likelihood of resulting in real actionable changes for patients and their families. Additionally, without the profit limitations of large drug corporations, patient-directed research allows for research in even unprofitable or otherwise marginalized areas.

In fact, the use of POSOMS promises to provide scientists with new and novel ways of collecting heretofore hard-to-collect data related to diseases, including for example, otherwise very expensive, hard-to-find, and hard-to-collect data on off-label usage of pharmaceuticals.[221] This is not necessarily a bad thing.[222] Some would argue that collecting data directly from patients, often in real time as they interact with the social media site, results in fewer concerns about the veracity of data,[223] particularly as a result of memory bias.[224]

Moreover, the use of patient reported data, particularly from POSOMS, can make expensive and time consuming off-label and new-use studies for existing drugs feasible.[225] POSOMS have also been helpful in locating otherwise lost patients in long-term longitudinal studies.[226]

There are some downsides to patients collectively becoming more involved in their research, particularly outside of normal

---

Jurgenson, *Production, Consumption, Prosumption: The Nature of Capitalism in the Age of the Digital "Prosumer"*, 10 J. CONSUMER CULTURE 13 (2010).

220. Effy Vayena & John Tasioulas, *The Ethics of Participant-Led Biomedical Research*, 31 NATURE BIOTECHNOLOGY 786 (2013).

221. Jeana Frost et al., *Patient-Reported Outcomes as a Source of Evidence in Off-Label Prescribing: Analysis of Data From PatientsLikeMe*, 13 J. MED. INTERNET RES., Jan.—Mar. 2011.

222. *See* Dina Fine Maron, *Your Medical Records May Unlock Disease Secrets for All*, SCI. AM. (August 6, 2015), *available at* http://www.scientificamerican.com/article/your-medical-records-may-unlock-disease-secrets-for-all/.

223. Paul Wicks et al., *Accelerated Clinical Discovery Using Self-Reported Patient Data Collected Online and a Patient-Matching Algorithm*, 29 NATURE BIOTECHNOLOGY 411 (2011).

224. Jeana H. Frost, *The Case for Using Social Media to Aggregate Patient Experiences with Off-Label Prescriptions*, 11 EXPERT REV. PHARMACOECONOMICS & OUTCOMES RESEARCH 371 (2011).

225. Frost, *supra* note 221.

226. Allison Cook Reaves & Diana W. Bianchi, *The Role of Social Networking Sites in Medical Genetics Research*, 161 AM. J. MED. GENETICS PART A 951 (2013).

operating parameters: for example, in one case a large cohort from a study colluded on Patientslikeme.com to determine who was receiving a placebo and who was receiving the actual drug over the course of a double-blind study, this sort of revelation can seriously harm the integrity of an expensive drug study.[227]

Other concerns include issues of selection bias (data population does not accurately reflect the actual broader patient population), confounding (misleading associations resulting from, for example, a third unrelated piece of information) and information bias (related to systematic errors associated with the collection of the data), resulting with, at minimum, that patient provided data collected through POSOMS out to be read and interpreted with a certain degree of caution.[228] Moreover, patient-led research lacks many of the built-in checks and balances of institutional-based research. For example, patient-led research typically does not carry the same ethical oversight; institutional review boards (IRBs) are typically lacking or privately financed in citizen science endeavors. (Some have also suggested that the same model that provides for patient led research, could also provide for patient-led or otherwise crowdsourced ethical review boards.[229])

Further, patient led research includes other ethical and scientific concerns including, lack of state recognition and support, issues related to the veracity and reliability of self-reported results,[230] general concerns with self-experimentation, inability to appreciate the risks of their own research, and the general blurring of the lines between researchers, subjects and sponsors, potentially a lack of openness and transparency and lack of informed consent.[231] Some have further argued that this patient-led "disobedience" against the institutionalized research system, while enabling rapid dissemination of research results and perhaps a greater degree of self-knowledge, nevertheless wades into ethically murky areas by short-circuiting

---

227. Virginia Hughes, *Social Storm: The Drug Industry is Struggling to Find Ways of Engaging with Consumers on Social Media*, 33 NATURE BIOTECHNOLOGY 14 (2015).

228. A. Cecile JW Janssens & Peter Kraft, *Research Conducted Using Data Obtained Through Online Communities: Ethical Implications of Methodological Limitations*, 9 PLOS MED. (2012).

229. *See, e.g.,* Melanie Swan, *Scaling Crowdsourced Health Studies: The Emergence of a New Form of Contract Research Organization*, 9 PERSONALIZED MED. 223 (2012).

230. Frost, *supra* note 221.

231. Effy Vayena, *Opinion: Unconventional Standards*, THE SCIENTIST (Mar. 13, 2013), *available at* http://www.the-scientist.com/?articles.view/articleNo/34690/title/Opinion—-Unconventional-Standards/.

standard pathways to review ethical concerns as well as informed consent.[232]

c. Suggestions For Regulation

With nearly 300,000 members on Patientslikeme.com alone,[233] not to mention the tens if not hundreds of other sites, actively policing these sites is not really feasible.

Nevertheless, patient oriented social media sites need some sort of regulatory oversight, not least because they involve a captured, desperate, and perhaps naïve community that can be easily taken advantage of.

As described above, concerns particularly come into play when patients are approached by health care workers or their doctors on these types of sites. These concerns are particularly apropos when these approaches are through thread initiators, individuals who tend to have substantial sway on these social media sites.[234] While some might argue that these sorts of interactions are important to humanize the doctors and open up otherwise stifled channels,[235] others are wary of inappropriate and/or illegal patient-doctor relationships,[236, 237] with some setting some important ground rules for these types of relationships.[238] In particular, social media interactions between doctors and patients raise these and other concerns: whether a doctor's particular opinion in one of these forums, intended narrowly may be misconstrued in a broader sense; difficulties in maintaining patient and colleague privacy; and whether the relaxed atmosphere

---

232. Paul Wicks et al., *Subjects No More: What Happens When Trial Participants Realize They Hold the Power?*, BRIT. MED. J. (2014), http://www.bmj.com/content/348/bmj.g368.full.pdf.

233. *Patients*, PATIENTSLIKEME, http://www.patientslikeme.com/patients (last visited Nov. 1, 2015).

234. Kordzadeh et al., *supra* note 128.

235. Sachin H. Jain, *Practicing Medicine in the Age of Facebook*, 361 NEW ENG. J. MED. 649 (2009).

236. Lori Wiener et al., *To Friend or Not to Friend: The Use of Social Media in Clinical Oncology*, 8 J. ONCOLOGY PRACTICE 103 (2012).

237. Paul H. Keckley & Michelle Hoffmann, *Social Networks in Health Care: Communication, Collaboration and Insights*, UNIVERSITY OF CALIFORNIA, SAN FRANCISCO (2010), https://www.ucsf.edu/sites/default/files/legacy_files/US_CHS_2010SocialNetworks_070710.pdf.

238. Manik S. Kadam & Murtaza M. Junaid Forooque, *Usage of Social Networking amongst Health-Care Professional for Dissemination of Medical Knowledge and Community Service*, RESEARCH GATE (June 16, 2015), *available at* http://www.researchgate.net/publication/277557656_Usage_of_Social_Networking_amongst_Health-Care_Professional_for_Dissemination_of_Medical_Knowledge_and_Community_Service.

may lead a professional to misrepresent science, medicine or their institutions or the nature of their degree and/or specialty. Nevertheless these sites remain practical additions to regular health care visits, with physician participation online most rewarding for underserved communities and geographically mobile patients.[239]

Other issues related to POSOMs relate generally to the generation and use of the patient and personal data on the websites. Who owns the data? Who is responsible for the accuracy of the patient's data and any data presented to the patient through the website, other members (e.g., patients and family) participating on the website and/or third parties? Who can access the data? Who is responsible for protecting and validating the data?[240]

In contrast to MMAs, a technological solution may not be best. In fact, with enforced proper disclosures, many of the concerns raised become mute. The problem lies in enforcing that disclosure and/or educating the often naïve consumer.

One solution might include a multi-tiered approach based on a certification that could be displayed on the websites' homepages. Thus, whatever governmental agency or non-governmental group takes it upon themselves to police these sites, that group/agency would make it known immediately to all visitors whether or not the site is in compliance with best practices or not. In addition to the certification mark, a concerted effort ought to be made to inform the doctors to educate their patients, if nothing else, to at least be wary and suspicious of their online interactions, even in their perceived safe environments of their online communities.

To this end, the policing body would be developed, perhaps in conjunction with patient groups, industry groups and other related agencies. Importantly, a set of best practices for all aspects of running the website, taking into account the needs and concerns of all stakeholders could be developed. This would include best practices relating to health-care worker anonymity, anonymizing data, advertising, selling data, patient interactions, physician interactions, pharmaceutical industry interactions and other relevant areas of concern. For example, physicians should be required to be non-anonymous with their credentials vetted. Similarly, pharmaceutical

---

239. Gemma Sinead Ryan, *Online Social Networks for Patient Involvement and Recruitment in Clinical Research*, 21 NURSE RESEARCHER 35 (2013).

240. Wei Wan-Chu, *Ethical Risks Inhabited in Social Networking Sites: A Case Study on PatientslikeMe.com*, INT'L PROC. COMPUTER SCI. & INFO. TECH. (2012), http://www.ipcsit.com/vol45/049-ICIKM2012-M20007.pdf.

companies and their agents would have to be clearly identified or risk being banned from the site. Perhaps something akin to Amazon's Real Name Badge program in customer reviews.[241] Additionally, patients should have to be fully informed in a clear and industry-wide consistent manner as to what happens to their data. Moreover, sites should employ the necessary technologies to prevent the wholesale scraping of data, as well as limiting non-member access to non-privileged areas.

Best practices would be suggested industry wide with certification seals from the oversight /policing group only provided to those websites that subscribe to all the best practices. Perhaps the same oversight/policing group could employ monitors to check up, unannounced, on a semi regular basis to review protocols, obtain data about problematic instances (e.g., an unidentified doctor, an individual masquerading as a doctor, defamation, or promotion of off-label uses by pharmaceuticals) and confirm that the website dealt with these issues as per best practices and protocol.

National and/or regional IRBs should also be created, not only would these be of value to many institutions that do not have the knowledgebase to create their own multidisciplinary IRBs, but also for citizen science resulting from patient oriented social media sites. Currently, most sites have to rely on expensive and sometimes ethically-conflicted paid-for services. Moreover the control and ownership of any drugs or technologies resulting from the citizen science or patient disclosures should be clearly explained to all participants, such that the websites do not unknowingly or secretly profit off of their member's efforts.

CONCLUSION

This paper presents two different but very much related emerging technologies: (1) mobile medical device applications that take advantage of the growing complexity of every day devices, and (2) patient oriented social media that builds off of the exponential growth of Web 2.0.

Both of these technologies (as employed particularly to the portion of the population with chronic diseases) can be extremely valuable, not only in providing information, support and care to those who need it, but also in efficiently creating data for the patients and

241. ABOUT BADGES, http://www.amazon.com/gp/help/customer/display.html/ref=cm_dly_lnk?ie=UTF8&nodeId=14279681&pop-up=1 (last visited Nov. 1, 2015).

their peers. Both technologies further serve to democratize what has traditionally been a paternalistic area of medical care. And, both technologies can be particularly helpful for the underserved and underrepresented in society.

Both also present significant challenges in that they can be easily abused, but not easily policed and regulated. To this end, this paper takes two very different approaches, suggesting that MMAs be less heavily regulated than they currently are, to promote innovation, and that POSOMS be more heavily regulated to protect their patient populations.

Many of the concerns raised with regard to MMAs can be better resolved with technological solutions that limit error and protect privacy. Whereas many of the concerns raised with regard to POSOMS require human intervention and oversight and cannot easily be addressed through implementing technological fixes.