GOING ROGUE: MOBILE RESEARCH APPLICATIONS AND THE RIGHT TO PRIVACY

*Stacey A. Tovino**

Introduction

Consider a hypothetical involving a woman with a progressive neurological condition.[1] The woman, who wishes to advance the scientific understanding of her condition, volunteers to participate in a disease-progression research study led by an independent scientist.[2] The research study requires each participant to download and use a mobile application ("mobile app") that was designed by the independent scientist and that collects a number of data elements, including first and last name, date of birth, race, ethnicity, diagnosis, medications, family history, and real-time information regarding balance, gait, vision, cognition, and other measures of disease progression.[3]

* Judge Jack and Lulu Lehman Professor of Law, William S. Boyd School of Law, University of Nevada, Las Vegas; J.D., University of Houston Law Center; Ph.D., University of Texas Medical Branch. This Article is an outgrowth of my participation as a research author on a grant project ("Addressing the Ethical, Legal, and Social Issues in Unregulated Health Research Using Mobile Devices") funded by the National Institutes of Health. I thank Principal Investigators Mark Rothstein and John Wilbanks for the opportunity to serve as a research author on this grant and to learn from their significant work on this topic. I also thank the participants of the "Data Min(d)ing: Privacy and Our Digital Identities" symposium held at the Federal Department of Health and Human Services in Washington, D.C., on October 22, 2018, for their comments and suggestions on the ideas presented in this Article. Finally, I thank Lena Rieke, Fellow, Wiener-Rogers Law Library, William S. Boyd School of Law, for her outstanding research assistance.

1 *See generally* Robin Ray & Anne Kavanagh, *Principles for Nursing Practice: Parkinson's Disease, Multiple Sclerosis and Motor Neurone Disease*, *in* Living with Chronic Illness and Disability 301 (Esther Chang & Amanda Johnson eds., 3d ed. 2018) (discussing progressive neurological conditions).

2 *See, e.g.*, Carrie Arnold, *Going Rogue*, Science (May 17, 2013), https://www.sciencemag.org/careers/2013/05/going-rogue (reporting the story of Ethan Perlstein, an independent scientist who engages in scientific research without affiliation to a university, pharmaceutical company, research institute, or government agency and without public funding).

3 *See generally* Sarah Moore et al., *Consent Processes for Mobile App Mediated Research: Systematic Review*, J. Med. Internet Res. mHealth & uHealth, Aug. 2017, at 3, https://

Assume that, during the research study, the independent scientist decides to share the participants' identifiable data with other researchers worldwide without the participants' prior notification or authorization.[4] Further assume the scientist sells the participants' names, addresses, and diagnoses to a healthcare marketing company, also without the participants' prior notification or authorization.[5] Moreover, assume a hacker accesses the participants' data as the data travels from the participants' smartphones to the scientist's contracted, backend data collector,[6] resulting in additional, unauthorized disclosures of the participants' identifiable data.[7] Finally, assume the scientist neither notifies the participants of these unauthorized disclosures nor provides instructions to the participants regarding how they can minimize potential economic, dignitary, and psychological harms associated with the unauthorized disclosures.[8]

Although hypothetical, this fact pattern is based on several recent enforcement actions[9] involving healthcare providers that failed to maintain

---

mhealth.jmir.org/2017/8/e126/ (discussing Apple's ResearchKit and Android's ResearchStack, two open-source frameworks that any scientist can use to create a mobile research app); *ResearchKit and CareKit*, APPLE, https://www.apple.com/researchkit/ (last visited Aug. 31 2019) (listing more than a dozen mobile research apps designed using ResearchKit); *About the Study*, MPOWER, https://parkinsonmpower.org/about (last visited Aug. 31, 2019) (describing a mobile-app-mediated research study that monitors the symptoms and progression of Parkinson's disease).

4 *See generally* Moore et al., *supra* note 3, Multimedia Appendix 1, Excel sheet *Confidentiality*, col. L *Open Data Sharing for Scientific Discovery*, https://mhealth.jmir.org/api/download?filename=FE0f53d825af51a87c76412316cee8cd.xlsx&alt_name=7014-105713-1-SP.xlsx (last visited Oct. 27, 2019) (noting that some mobile-app-mediated researchers share research data with researchers outside the primary research team as well as with qualified researchers worldwide).

5 *See, e.g.*, Bonnie Kaplan, *Selling Health Data: De-Identification, Privacy, and Speech*, 24 CAMBRIDGE Q. HEALTHCARE ETHICS 256 (2015) (discussing privacy and other legal issues raised by the sale of health data); I. Glenn Cohen & Michelle M. Mello, *Big Data, Big Tech, and Protecting Patient Privacy*, 322 JAMA 1141 (2019) [hereinafter, Cohen & Mello, *Big Data*] (discussing the market for health data).

6 *See, e.g.*, Moore et al., *supra* note 3, Multimedia Appendix. 1, Excel sheet *Confidentiality*, col. H *Backend Collector*, https://mhealth.jmir.org/api/download?filename=FE0f53d825af51a87c76412316cee8cd.xlsx&alt_name=7014-105713-1-SP.xlsx (noting that some mobile-app-mediated researchers contract with a third party to provide backend data collection services).

7 *See, e.g.*, Douglas Busvine & Stephen Nellis, *Security Flaws Put Virtually All Phones, Computers at Risk*, REUTERS (Jan. 3, 2018), https://finance.yahoo.com/news/security-flaws-put-virtually-phones-035449033.html (discussing security flaws that allow hackers to steal sensitive information from smart phones).

8 *Compare* 45 C.F.R. § 164.404(a)(1) (2018), *with id.* § 164.404(c)(1) (requiring HIPAA-covered entities, following the discovery of a breach of unsecured protected health information (uPHI), to notify each individual whose uPHI has been, or is reasonably believed to have been, accessed, acquired, used, or disclosed as a result of the breach).

9 *See, e.g.*, U.S. DEP'T HEALTH & HUMAN SERVS., RESOLUTION AGREEMENT WITH MANAGEMENT SERVICES ORGANIZATION WASHINGTON, INC. 1–2 (2010), https://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/msoresagr.html (requiring Management Services Organization Washington, Inc. (MSO) to pay HHS $35,000 following MSO's unau-

the privacy and security of individually identifiable health information collected during clinical encounters, thereby violating applicable federal privacy, security, and breach notification rules ("Rules") that implement the administrative simplification provisions within the Health Insurance Portability and Accountability Act (HIPAA) of 1996, as amended by the Health Information Technology for Economic and Clinical Health Act (HITECH).[10] As background, the HIPAA Rules were designed to protect the privacy and security of individually identifiable health information created or maintained in the healthcare and health insurance contexts and to assist patients and insureds in protecting themselves in the event of a privacy or security breach.[11] Although HIPAA authorizes the federal government to impose civil and criminal penalties for violations of the HIPAA Rules,[12] the HIPAA Rules are limited in application to (1) health plans, healthcare clearinghouses, and those healthcare providers that transmit health information in electronic form in connection with standard transactions, including health

thorized disclosure of electronic PHI (ePHI) for marketing purposes); U.S. DEP'T HEALTH & HUMAN SERVS., RESOLUTION AGREEMENT WITH MEMORIAL HERMANN HEALTH SYSTEM 1–2 (2017), https://www.hhs.gov/sites/default/files/mhhs_ra_cap.pdf (requiring Memorial Hermann Health System ("Memorial") to pay $2.4 million to the Federal Department of Health and Human Services (HHS) following Memorial's unauthorized disclosure of protected health information (PHI)); U.S. DEP'T HEALTH & HUMAN SERVS., RESOLUTION AGREEMENT WITH METRO COMMUNITY PROVIDER NETWORK 1–2 (2017), https://www.hhs.gov/sites/default/files/mcpn-ra-cap.pdf (requiring Metro Community Provider Network ("Metro") to pay HHS $400,000 following Metro's failure to implement policies and procedures designed to prevent, detect, contain, and correct security violations, thereby allowing a hacker to access the ePHI of 3200 Metro patients); U.S. DEP'T HEALTH & HUMAN SERVS., RESOLUTION AGREEMENT WITH PRESENCE HEALTH NETWORK 1–2, 4 (2017), [hereinafter PRESENCE RESOLUTION AGREEMENT], https://www.hhs.gov/sites/default/files/presence-ra-cap.pdf (requiring Presence Health Network ("Presence") to pay HHS $475,000 following Presence's failure to timely notify individuals of the breach of their uPHI).

10 *See* Health Insurance Portability and Accountability Act (HIPAA) of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (codified as amended in scattered titles of the U.S Code), *amended by* Health Information Technology for Economic and Clinical Health Act (HITECH), Pub. L. No. 111-5, 123 Stat. 226 (2009) (codified as amended in scattered sections of 42 U.S.C.). HHS's privacy regulations, which implement section 264(c) of HIPAA, are codified at 45 C.F.R. §§ 164.500–.534 [hereinafter HIPAA Privacy Rule]. HHS's security regulations, which implement section 262(a) of HIPAA (42 U.S.C. § 1320d–2(d)(1)), are codified at 45 C.F.R. §§ 164.302–.318 [hereinafter HIPAA Security Rule]. HHS's breach notification regulations, which implement section 13402 of HITECH (42 U.S.C. § 17932), are codified at 45 C.F.R. §§ 164.400–.414 [hereinafter HIPAA Breach Notification Rule].

11 *See* 45 C.F.R. §§ 164.500–.534, .302–.318, .400–.414 (setting forth the privacy, security, and breach notification obligations of covered entities and business associates under the HIPAA Rules).

12 *See* 42 U.S.C. § 1320d-6 (2012) (establishing criminal penalties for violations of the HIPAA Rules); HIPAA, *supra* note 10, § 242 (establishing civil penalties for violations of the HIPAA Rules); and HITECH, *supra* note 10, § 13410(d) (revising the amount of the civil penalties authorized by HIPAA).

insurance claims ("covered entities");[13] and (2) persons or entities that access or use protected health information (PHI) to provide certain services to, or to perform certain functions on behalf of, covered entities ("business associates").[14]

The HIPAA Rules do not regulate a number of individuals and institutions that collect, use, or disclose individually identifiable health information, including many independent scientists,[15] citizen scientists,[16] and patient researchers,[17] as well as some mobile-app developers and data storage companies that support them.[18] As a result, the voluminous and diverse data

13 *See* 45 C.F.R. § 160.103 (2018) (defining covered entity); *id.* § 160.102(a) (applying the HIPAA Rules to covered entities).

14 *See id.* § 160.103 (defining business associate); *id.* § 160.102(b) (applying the HIPAA Rules to business associates).

15 *See, e.g.*, Amber Dance, *Solo Scientist*, 543 NATURE 747, 747–49 (2017) (reporting the story of Jeffrey Rose, an independent scientist who conducts research "without the benefits of a conventional, bricks-and-mortar employer").

16 *See, e.g.*, Lisa M. Rasmussen, *When Citizens Do Science: Stories from Labs, Garages, and Beyond*, 9 NARRATIVE INQUIRY BIOETHICS 1, 1–4 (2019) (providing background information regarding the conduct of citizen science); Mark A. Rothstein et al., *Citizen Science on Your Smartphone: An ELSI Research Agenda*, 43 J.L. MED. & ETHICS 897, 897 (2015) (explaining that the term citizen scientist originally referred to "non-professionals assisting professional scientists by contributing observations and measurements to ongoing research enterprises"; also explaining that the term "now includes nonprofessionals who conduct scientific experiments of their own design independent from professional scientists"—clarifying that citizen science has been made possible by "online crowdsourcing, big data capture strategies, and computational analytics," among other technological developments); Todd Sherer, *Parkinson's Disease at 200*, SCI. AM. (Apr. 12, 2017), https://blogs.scientificamerican.com/guest-blog/parkinsons-disease-at-200/ (referencing technology that citizens use to participate in research investigating Parkinson's disease).

17 *See, e.g.*, Paul Wicks et al., *Accelerated Clinical Discovery Using Self-Reported Patient Data Collected Online and a Patient-Matching Algorithm*, 29 NATURE BIOTECH. 411, 411–14 (2011) (analyzing data reported on a website by patient researchers with ALS who experimented with lithium carbonate).

18 *See, e.g.*, Cohen & Mello, *Big Data*, *supra* note 5, at 231 ("HIPAA is a 20th-century statute ill equipped to address 21st-century data practices."); I. Glenn Cohen & Michelle M. Mello, *HIPAA and Protecting Health Information in the 21st Century*, 320 JAMA 231, 232 (2018) [hereinafter Cohen & Mello, *HIPAA*] ("HIPAA 'attaches (and limits) data protection to traditional health care relationships and environments.' The reality . . . is that HIPAA-covered data form a small and diminishing share of the health information stored and traded in cyberspace." (footnote omitted) (quoting Nicolas P. Terry, *Big Data Proxies and Health Privacy Exceptionalism*, 24 HEALTH MATRIX 65, 69 (2014))); Rothstein et al., *supra* note 16, at 899 ("[R]esearch undertaken by an individual or entity that is not a HIPAA-covered entity, such as a citizen scientist, is not required to follow federal privacy rules."); Mark A. Rothstein, *The End of the HIPAA Privacy Rule?* 44 J.L. MED. & ETHICS 352, 352 (2016) ("Among the reasons for the Privacy Rule's disrepute, especially among privacy advocates, is its limited coverage; it applies only to 'covered entities' . . . ."); Nicolas P. Terry & Tracy D. Gunter, *Regulating Mobile Mental Health Apps*, 36 BEHAV. SCI. & L. 136, 139–40 (2018) ("[Mobile medical applications] tend to be developed outside of traditional healthcare spaces with the result that they exist in a lightly regulated, 'HIPAA-free zone.'" (citation omitted)).

collected by some independent scientists who use mobile apps to conduct health research may be at risk for unregulated privacy and security breaches,[19] leading to dignitary, psychological, and economic harms for which the participants have few legally enforceable rights or remedies.[20]

Many academic and practitioner discussions regarding health-related big data have suggested new federal laws or amendments to existing federal laws in an attempt to create comprehensive privacy and security protections for otherwise unprotected data.[21] It is not clear, however, that the federal government has the desire or capacity to enforce expanded or new laws in this area. In a recent study, for example, the author found that a timely filed consumer complaint involving an actual violation of the HIPAA Rules over which the Office for Civil Rights within the Federal Department of Health and Human Services (HHS) has jurisdiction has a one-tenth of one percent (0.1%) chance of triggering a settlement or civil money penalty.[22] The author also showed that in those few cases that go to settlement or penalty, the federal government takes a significant amount of time—more than seven years in some cases—to execute the settlement agreement or to impose the

19 *See, e.g.*, Opperman v. Path, Inc., 205 F. Supp. 3d 1064, 1073 (N.D. Cal. 2016) (explaining that the mobile app Yelp exceeded the scope of its users' consent when it uploaded its users' contacts data without explicit permission); Zeynep Tufekci, *The Latest Data Privacy Debacle*, N.Y. Times (Jan. 30, 2018), https://www.nytimes.com/2018/01/30/opinion/strava-privacy.html?rref...ule=stream_unit&version=search&contentPlacement=3&pgtype=collection (reporting on the mobile exercise app Strava, which inadvertently revealed the secret locations of American military bases and service members).

20 *See, e.g.*, Mark A. Rothstein, *Ethical Issues in Big Data Health Research*, 43 J.L. Med. & Ethics 425, 426–27 (2015) (discussing physical and dignitary harms associated with the loss of privacy in the context of big-data health research).

21 *See, e.g.*, Cohen & Mello, *HIPPA*, *supra* note 18, at 232 (noting that federal options include expanding the application of the HIPAA Rules and crafting new federal legislation); Lawrence O. Gostin et al., *Health Data and Privacy in the Digital Era*, 320 JAMA 233, 234 (2018) (referencing federal guidance that could be expanded to apply to mobile-app developers and social media); James Swann, *Your Fitbit Steps May Not Be Protected by Federal Law*, Bloomberg L. (May 30, 2018) ("It's almost certain that the federal government will look to regulate health information that's not subject to HIPAA, Thora Johnson, a [prominent] health-care attorney . . . , told Bloomberg Law."). A number of data privacy and/or security bills that would expand HIPAA or create new legislation have recently been introduced to Congress. As of this writing, however, not one has been enacted. *See, e.g.*, Protecting Personal Health Data Act, S. 1842, 116th Cong. (2019) (directing the HHS Secretary to promulgate regulations to help strengthen privacy and security protections for consumers' personal health data that is collected, processed, analyzed, or used by consumer devices, services, applications, and software); Data Care Act of 2018, S.3744, 115th Cong., § 3 (2018) (establishing duties of "care, loyalty, and confidentiality" for online service providers that handle personal data). A number of voluntary data privacy and security guidelines have also been recently released for the health industry. *See, e.g.*, U.S. Dep't Health & Human Servs., Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients (2018), https://www.phe.gov/Preparedness/planning/405d/Documents/HICP-Main-508.pdf (describing voluntary cybersecurity practices for health care organizations of all types and sizes, including local clinics and large hospital systems).

22 Stacey A. Tovino, *A Timely Right to Privacy*, 104 Iowa L. Rev. 1361, 1406 (2019).

civil money penalty.[23] The author concluded that the federal desire and capacity to enforce the HIPAA Rules appear to be low, resulting in a lack of timely attention to the privacy and security rights of individuals.[24]

This Article furthers this line of research by investigating whether nonsectoral state laws may serve as a viable source of privacy and security standards for mobile health research participants and other health data subjects until new federal laws are created or enforced. In particular, this Article (1) catalogues and analyzes the nonsectoral data privacy, security, and breach notification statutes of all fifty states and the District of Columbia; (2) applies these statutes to mobile-app-mediated health research conducted by independent scientists, citizen scientists, and patient researchers; and (3) proposes substantive amendments to state law that could help protect the privacy and security of all health data subjects, including mobile-app-mediated health research participants.[25]

This Article proceeds as follows: Part I provides background information regarding mobile apps and their use by independent scientists, citizen scientists, and patient researchers as well as conventional researchers who fall outside traditional sources of privacy and security regulation. After reviewing federal and international data privacy, security, and breach notification standards, Part II shows why some citizen scientists, independent researchers, and patient researchers, as well as the mobile-app developers and data storage and processing companies that support them, are not subject to such regulation.

Part III of this Article reports the results of a comprehensive survey of state privacy, security, and breach notification laws. In particular, Part III investigates the presence or absence in the statutes of each state and the District of Columbia of nonsectoral data privacy and security standards, including prior notification of and authorizations for the use and disclosure of individually identifiable data; administrative, technical, and physical data

23 *See id.*

24 *See id.*

25 Prior legal scholarship relating to mobile health research and independent science has focused on the lack of application of federal and state health industry and health research standards. *See, e.g.*, Stacey A. Tovino, *Mobile Research Applications and State Research Laws*, J.L. MED. & ETHICS (forthcoming 2019); Stacey A. Tovino, *Privacy and Security Issues in mHealth Research*, J.L. MED. & ETHICS (forthcoming 2019); Mark A. Rothstein, John T. Wilbanks, Laura M. Beskow, Kathleen M. Brelsford, Kyle B. Brothers, Megan Doerr, Catherine M. Hammack, Michelle L. McGowan & Stacey A. Tovino, *Unregulated Health Research Using Mobile Devices: Ethical Considerations and Policy Recommendations*, J.L. MED. & ETHICS (forthcoming 2019). Prior scholarship examining mobile health apps generally tends to focus on mobile health app quality, safety, and efficacy. *See, e.g.*, Natalie R. Bilbrough, Comment, *The FDA, Congress, and Mobile Health Apps: Lessons from DSHEA and the Regulation of Dietary Supplements*, 74 MD. L. REV. 921 (2015) (discussing mobile health app malfunction, substandard health advice, and potential physical harms); Saabira Chaudhuri, *Fertility Apps Are Multiplying. But Are They Reliable?*, WALL ST. J. (May 24, 2018), https://www.wsj.com/articles/fertility-apps-are-multiplying-but-are-they-reliable-1527182930 (questioning the efficacy of mobile fertility apps).

safeguards; and breach notification to individuals, government agencies, and consumer reporting agencies. Part III applies these rights and protections, when they exist, to individuals who conduct and support mobile-app-mediated health research. Part III finds that all jurisdictions have at least one potentially applicable breach notification statute, more than two-thirds of jurisdictions have at least one potentially applicable data security statute, and more than one quarter of jurisdictions have at least one potentially applicable data privacy statute. These findings suggest that states have the current or potential infrastructure to protect the privacy and security of mobile health research data and other health-related data that is not protected by traditional, federal health laws such as the HIPAA Rules.

Taking a nonsectoral approach to data privacy and security, this Article concludes by proposing amendments to breach notification statutes as well as content for states that lack generally applicable data privacy and security statutes. If adopted, these proposals could create cross-industry privacy and security protections that will benefit all health data subjects, including participants in mobile-app-mediated health research. This Article also considers the challenges and opportunities associated with both intra- and interindustry data privacy and security regulation. Although sectoral approaches to privacy and security made sense even a quarter of a century ago, the time has come for generally applicable forms of data protection.

I. Health Research and Mobile Applications

Mobile apps are a fast-growing category of software typically installed on personal smartphones and wearable devices.[26] Used for a wide range of health-related activities, including fitness, health education, health prediction, diagnosis, healthcare delivery, treatment support, chronic disease management, health research, disease surveillance, and epidemic-outbreak tracking, among other activities, mobile apps have tremendous versatility and promise.[27] Mobile apps are currently used in almost every area of medicine

26 *See, e.g.*, Terry & Gunter, *supra* note 18, at 136 (providing background information regarding mobile health apps).

27 *See, e.g.*, Valerie Gay & Peter Leijdekkers, *Bringing Health and Fitness Data Together for Connected Health Care: Mobile Apps as Enablers of Interoperability*, 17 J. Med. Internet Res. 37 (2015), http://www.jmir.org/2015/11/e260/ (discussing fitness and health uses of mobile apps as well as the aggregation of such uses); Deborah Lupton & Annemarie Jutel, *'It's Like Having a Physician in Your Pocket!' A Critical Analysis of Self-Diagnosis Smartphone Apps*, 133 Soc. Sci. & Med. 128, 128–35 (2015) (analyzing diagnostic uses of mobile apps, including the effects such apps have on the physician-patient relationship and medical authority in relation to diagnosis); Elaine O. Nsoesie et al., *New Digital Technologies for the Surveillance of Infectious Diseases at Mass Gathering Events*, 21 Clinical Microbiology & Infection 134, 134–140 (2015) (focusing on disease surveillance uses of mobile apps and other digital technologies); Ben Underwood et al., *The Use of a Mobile App to Motivate Evidence-Based Oral Hygiene Behaviour*, 219 Brit. Dental J. E2 (2015) (reporting the results of a study assessing user perceptions of an oral health app that provides education and behavioral support related to oral health).

and health, including dermatology,[28] maternal, newborn, and child health,[29] and communicable and contagious diseases,[30] just to name a few.

This Article focuses on the use of mobile apps for health-related research, concentrating in particular on mobile-app-mediated research conducted or participated in by independent scientists, citizen scientists, and patient researchers. As background, an independent scientist, also known as a rogue or lone scientist, is an individual who engages in scientific research without affiliation to a university, hospital, pharmaceutical company, research institute, government agency, or other third party.[31] A citizen scientist, also known as a community scientist, crowd scientist, or amateur scientist, is a member of the general public who engages in scientific work, sometimes in collaboration with or under the direction of a professional, affiliated scientist, and the scientist's academic or other institution.[32] Citizen scientists also include non–professionally trained scientists who independently conduct their own experiments, frequently with the assistance of mobile apps, online crowdsourcing, computational analytics, and other technologies made possible by big data.[33] A patient researcher is a current or former patient who initiates or assists research at any stage of the research process, including establishing the research agenda, designing the research protocol, collecting data, or disseminating research results.[34] Mobile apps have been tremendously helpful to independent scientists, citizen scientists, and patient researchers, as well as conventional scientists who fall outside traditional regulation (collectively, independent scientists), in the conduct of a wide range

28 *See, e.g.*, Ann Chang Brewer et al., *Mobile Applications in Dermatology*, 149 JAMA DERMATOLOGY 1300, 1300–04 (2013) (identifying and categorizing 209 unique dermatology-related mobile apps).

29 *See, e.g.*, Francis Dzabeng et al., *Community Health Workers' Experiences of Mobile Device-Enabled Clinical Decision Support Systems for Maternal, Newborn and Child Health in Developing Countries: A Qualitative Systematic Review Protocol*, JBI DATABASE SYSTEMATIC REVIEWS & IMPLEMENTATION REP., Sept. 2016, at 57 (synthesizing evidence regarding the experiences of community health workers of "mobile device-enabled clinical decision support systems" interventions designed to support maternal, newborn, and child health in low- and middle-income countries).

30 *See, e.g.*, Jamie I. Forrest et al., *Mobile Health Applications for HIV Prevention and Care in Africa*, 10 CURRENT OPINION HIV & AIDS 464 (2015) (conducting a literature review of mobile health interventions for HIV prevention and care in Africa).

31 *See, e.g.*, James Lovelock, *We Need Lone Scientists*, INDEPENDENT (Mar. 26, 2014), https://www.independent.co.uk/life-style/health-and-families/features/james-lovelock-we-need-lone-scientists-9215280.html (comparing affiliated scientists, who work in large corporations or for the government, with lone (or independent) scientists who work alone in their own laboratories).

32 *Citizen Scientist*, OXFORD ENG. DICTIONARY, https://www.oed.com/view/Entry/33513?redirectedFrom=citizen+scientist#eid316597459 (defining citizen scientist).

33 *See* Rothstein et al., *supra* note 16, at 897 (explaining the development of the term citizen scientist).

34 *See generally* Jenny Leese et al., *Evolving Patient-Researcher Collaboration: An Illustrative Case Study of a Patient-Led Knowledge Translation Event*, 9 J. PARTICIPATORY MED. 3 (2017), https://jopm.jmir.org/2017/1/e13 (discussing patient engagement in research).

of health research projects.[35] Four illustrative mobile apps that involve independent scientists in one form or another are discussed below.

A. Kinsey Reporter

The Kinsey Reporter mobile apps, available for iOS in the Apple App Store and Android on Google Play, collect real-time, anonymous data about sexual health, sexual behaviors, and other intimate behaviors reported by their "citizen sex scientists."[36] Kinsey Reporter communicates the collected data to KinseyReporter.org, a global mobile platform designed by researchers based in Bloomington, Indiana, that aggregates, maps, and shares the data with the public.[37] Some of the data collected by Kinsey Reporter is quite sensitive. With respect to sexual health, collected data includes hormonal contraception use, methods, and effects, including irregular bleeding, vaginal dryness, missed menses, breast tenderness, severe headache, nausea, and anxiety.[38] With respect to unwanted sexual behavior, collected data includes reports of physical injuries as well as data confirming whether the recipient of the unwanted behavior reported the behavior to a legal authority.[39] Although Kinsey Reporter collects neither the name (nor any type of user identity) nor precise geolocation of its citizen sex scientists,[40] Kinsey Reporter does collect data regarding the city, state, and country (e.g., "Seminole, Florida, US") where the reported sexual health issue or intimate behav-

35 *See, e.g.*, Elizabeth Klemick, *Mobile Apps for Citizen Science*, SMITHSONIAN SCI. EDUC. CTR., https://ssec.si.edu/stemvisions-blog/mobile-apps-citizen-science (last visited Sept. 1, 2019) ("An abundance of mobile apps makes participation in citizen science projects easier than ever and allows data entry in the field.").

36 *See* Clayton A. Davis et al., Citizen Science for Sex Research 1 (Feb. 16, 2016) (unpublished manuscript), https://arxiv.org/pdf/1602.04878.pdf ("'Citizen sex scientists' submit reports, each consisting of one or more surveys, after participating in or observing sexual activity. Surveys cover topics such as flirting, sexual activity, unwanted experience, consumption of pornography, and hormonal birth control side effects."); *Kinsey Reporter*, APPLE, https://apps.apple.com/us/app/kinsey-reporter/id533205458 (last visited Aug. 28, 2019); *Kinsey Reporter*, GOOGLE, https://play.google.com/store/apps/details?id=com.kinsey.android (last visited Aug. 28, 2019).

37 *See Home*, KINSEY REPORTER, https://kinseyreporter.org/#/ (last visited Aug. 30, 2019).

38 *See Explore*, KINSEY REPORTER, https://kinseyreporter.org/#/explore (last visited Aug. 30, 2019) (depicting data about hormonal birth control use and effects).

39 *See id.* (depicting data about sexual aggression).

40 *See Privacy Policy*, KINSEY REPORTER, https://kinseyreporter.org/#/ (last visited Aug. 30, 2019) [hereinafter *Kinsey Reporter Privacy Policy*] (stating that the data collected and shared by Kinsey Reporter is anonymous); *id.* ("The Application does not collect or transmit detailed geolocation data from the GPS technology within your mobile device."). *See generally* Davis et al., *supra* note 36 (discussing the research goals of Kinsey Reporter); *Kinsey Reporter: Citizen Observers Report on Sexual Behavior and Experiences As Well As Share, Explore and Visualize the Accumulated Data*, SCI. AM. (Nov. 5, 2013), https://www.scientificamerican.com/citizen-science/kinsey-reporter/.

ior occurred, as well as the age, gender, and internet protocol (IP) address of the reporting citizen sex scientist.[41]

One of the stated goals of Kinsey Reporter is to reveal how sexual health, norms, and behaviors vary depending on geography.[42] Hormonal birth control, for example, reportedly affects women living in different geographic areas differently. To unpack those differences, Kinsey Reporter collects data regarding the effects of hormonal birth control together with the location of the reporting citizen sex scientist.[43] A second stated goal of Kinsey Reporter is to stimulate discussion regarding the challenges and opportunities associated with using citizen-science platforms to collect data about sensitive health issues and intimate behaviors.[44]

B. ActiveDay

Independent scientists use mobile apps to collect a wide variety of health-related data, not just data related to sexual health and intimate behavior. For example, the ActiveDay mobile app, available for iOS in the Apple App Store, was designed by Tidyware, LLC, for research on occupational-health-and-safety technology, including fall detection and prevention.[45] In particular, ActiveDay uses the sensors in its participating, citizen scientists' smartphones to monitor physical activity and detect irregular movements.[46] When ActiveDay detects an irregular movement, it sends a message to the citizen scientist asking whether the movement was caused by a fall or whether the citizen scientist was just walking or running or had simply dropped the citizen scientist's phone.[47] ActiveDay then sends the irregular movement and the citizen scientist's classification of the irregular movement to storage for research and development relating to occupational safety.[48] According

41 *Kinsey Reporter Privacy Policy*, *supra* note 40 ("The Application obtains the information you provide[, including] . . . survey responses; approximate date and time that the survey response is submitted; and the city, state/region, or country location that you designate when completing the survey."); *Explore: Top Surveys in Seminole, Florida, US*, KINSEY REPORTER, https://kinseyreporter.org/#/explore?country=2&state=75&city=376 (sharing data showing that a female data entrant located in Seminole, Florida, reported hormonal birth control use).

42 Davis et al., *supra* note 36, at 4 (explaining the importance of geography to the research study).

43 *Id.*

44 *Id.* at 2.

45 *ActiveDay—Activity Study*, APPLE, https://apps.apple.com/us/app/activeday-activity-study/id1183046259 (last visited Sep. 1, 2019) (describing the ActiveDay app).

46 *Id.* (describing the data gathered by ActiveDay).

47 Screenshot of Movement Detection Message from ActiveDay to Stacey Tovino (on file with author) (asking whether the user fell or dropped her phone, or whether she was walking or running, after she intentionally dropped her phone from the second floor of her house to the first floor).

48 *Active Day—Activity Study 2.0.2 License Agreement*, APPLE, https://apps.apple.com/us/app/activeday-activity-study/id1183046259 (follow "License Agreement") (last visited Oct. 13, 2019).

to ActiveDay's privacy policy, citizen scientists who use ActiveDay grant Tidyware and its successors, business affiliates, and independent contractors the permanent, irrevocable ability to use the collected data for research purposes relating to occupational health and safety.[49]

Tidyware is a small, privately held company located in Bellevue, Washington, incorporated under Washington law.[50] In addition to ActiveDay, Tidyware also owns and operates FallSafety Pro, a mobile app designed to protect the physical safety of individuals who work at height,[51] including painters, roofers, linemen, oil field workers, service technicians, framers, and window cleaners.[52] To this end, FallSafety Pro collects each app user's name, phone number, email address, and real-time GPS location, as well as the name, phone number, and email address of the individual's emergency contact. FallSafety Pro then uses hardware and software in each user's smart phone to detect whether the user has fallen and to provide GPS-enabled directions to emergency contacts and first responders in the event of a fall.[53] FallSafety Pro also collects data regarding the number of times each user has fallen.[54]

C. PatientsLikeMe

Kinsey Reporter and ActiveDay rely on citizen scientists who volunteer their data for sexual-health and occupational-safety research, respectively. In some mobile-app-mediated research studies, patients actually initiate and direct the research. Some background is necessary before proceeding with an example of this type of patient-led research. In 2008, a group of Italian scientists published the results of a small, pilot study investigating whether lithium, typically used as a mood stabilizer for patients with mental illness, may delay the progression of amyotrophic lateral sclerosis (ALS).[55] ALS is a

49 *Id.*

50 *Tidyware LLC*, MANTA, https://www.manta.com/c/mb42sxd/tidyware-llc (last visited Sep. 1, 2019) ("Tidyware LLC is a privately held company in Bellevue, WA [that was] . . . established in 2012 and incorporated in Washington. Current estimates show this company has an annual revenue of [$]204,157 and employs a staff of approximately 3.").

51 E-mail from Philip Carmichael, CEO of FallSafety, to Stacey Tovino, (May 31, 2018, 4:20 PM) (on file with author) ("Our team created FallSafety Pro specifically to address the safety needs of those who work at height. We've tuned the solution to detect larger falls and impacts, that occur on jobsites, while filtering out smaller events that could trigger false alarms.")

52 *How It Works*, FALLSAFETY, https://www.fallsafetyapp.com/how-it-works (last visited Sept. 1, 2019).

53 *See id.* After the app detects a possible fall, it gives the user forty-five seconds to respond and cancel the emergency response. *Id.* If the response is canceled, the user is asked questions to determine what triggered the app's motion detector; if the response is not canceled, the app notifies emergency personnel. *Id.*

54 *See Privacy Policy*, FALLSAFETY, https://www.fallsafetyapp.com/privacy (last visited Sept. 1, 2019) [hereinafter *FallSafety Privacy Policy*].

55 Francesco Fornai et al., *Lithium Delays Progression of Amyotrophic Lateral Sclerosis*, 105 PROC. NAT'L ACAD. SCI. 2052 (2008).

progressive neurodegenerative disease that affects nerve cells in the brain and the spinal cord and that typically leads to death within three to five years of diagnosis.[56] The authors of the small pilot study formally concluded that lithium does delay the progression of ALS in human patients.[57]

As news of the Italian study traveled, many patients with ALS wanted to try lithium to see if their disease progressions could be delayed. In particular, a group of 149 patients with ALS who had registered on a free, health data sharing website—PatientsLikeMe.com—obtained and then experimented with lithium carbonate off label for at least two months, although some patients experimented as long as twelve months.[58] Using an online, lithium-specific, data collection tool, the patients reported a number of data elements, including demographic data, site of ALS onset, lithium-treatment start and stop dates, and functional-impairment scores over time in the domains of speech, swallowing, walking, arm function, and respiratory function.[59] A published study, conducted internally at PatientsLikeMe, formally concluded that lithium had no effect on ALS disease progression at twelve months.[60] The study also suggested, however, that "data reported by patients over the internet may be useful for accelerating clinical discovery and evaluating the effectiveness of drugs already in use."[61]

The 149 ALS patients referenced above submitted their data to PatientsLikeMe using an online data collection tool, not a mobile app. However, PatientsLikeMe, which is headquartered in Cambridge, Massachusetts, has health data sharing apps available for iOS in the Apple App Store and Android on Google Play.[62] Using these apps, patients can share their data, including user identifications, photos, email addresses, demographic information, ages, ethnicities, races, diagnoses, genetic information, symptoms, laboratory results, and treatment regimes, among other data elements.[63] Indeed, registered users located in the United States, European Union, and

56 *See, e.g.*, *Amyotrophic Lateral Sclerosis (ALS) Fact Sheet*, NAT'L INST. NEUROLOGICAL DISORDERS & STROKE (June 2013), https://www.ninds.nih.gov/Disorders/Patient-Caregiver-Education/Fact-Sheets/Amyotrophic-Lateral-Sclerosis-ALS-Fact-Sheet (describing the disease).

57 *See* Fornai et al., *supra* note 55, at 2056 ("Our study indicates that lithium delays ALS progression in human patients.").

58 Wicks et al., *supra* note 17, at 411–14.

59 *Id.* at 411, 412 & fig.1.

60 *Id.* at 411 ("At 12 months after treatment, we found no effect of lithium on disease progression.").

61 *Id.*

62 *PatientsLikeMe*, APPLE, https://apps.apple.com/us/app/patientslikeme/id955272281 (last visited Aug. 30, 2019); *Patients Like Me*, GOOGLE, https://play.google.com/store/apps/details?id=com.patientslikeme.android&hl=EN_US (last visited Aug. 30, 2019); *see Contact Us*, PATIENTSLIKEME, https://www.patientslikeme.com/about/contact (last visited Aug. 30, 2019) (listing a Cambridge, Massachusetts, headquarters address).

63 *See* Jim Edwards, *PatientsLikeMe Is More Villain than Victim in Patient Data "Scraping" Scandal*, CBS NEWS (Oct. 18, 2010), https://www.cbsnews.com/news/patientslikeme-is-more-villain-than-victim-in-patient-data-scraping-scandal/ (listing the types of data elements collected by PatientsLikeMe).

other jurisdictions are currently sharing data with respect to more than 2800 health conditions, including sensitive and stigmatizing conditions such as colon cancer, genital herpes, HIV, obesity, paranoid schizophrenia, alcohol-use disorder, and drug-use disorder.[64] According to the app's privacy policy, PatientsLikeMe aggregates and organizes the data shared by its member patients and then reshares and/or sells it to universities, pharmaceutical companies, hospital systems, insurance companies, and regulatory bodies for research and other purposes.[65]

D. MyFitnessPal

Under Armour Inc. is an American apparel company that manufactures athletic footwear as well as sports and casual clothing.[66] Although Under Armour's global headquarters are located in Baltimore, Under Armour has a number of international offices, including in Amsterdam, Guangzhou, Hong Kong, Jakarta, London, Mexico City, Munich, Panama City, Paris, São Paulo, Santiago, Seoul, Shanghai, and Toronto.[67] Founded in 1996 by Kevin Plank, a former University of Maryland football player, Under Armour apparel is well known for keeping its users cool, dry, and stylish throughout the course of a game, practice, or workout.[68] In addition to apparel, however, Under Armour also owns and operates a number of mobile apps, including MyFitnessPal.[69] MyFitnessPal allows users to track their fitness and health by entering a wide range of health data relating to food, exercise, and body weight, as

64 *Conditions*, PATIENTSLIKEME, https://www.patientslikeme.com/conditions (last visited Aug. 30, 2019) ("Members are tracking more than 2,800 conditions on PatientsLike Me."); *Find Patients: Italy*, PATIENTSLIKEME, https://www.patientslikeme.com/patients/searches/detail_search (follow "Additional filters" under "Filter patients by:"; then follow "Italy" under "Country") (last visited Oct. 13, 2019) (showing that patients from Italy and other EU member states are sharing data).

65 *Does PatientsLikeMe Sell My Information?*, PATIENTSLIKEME, https://support.patientslikeme.com/hc/en-us/articles/201245770-Does-PatientsLikeMe-sell-my-information- (last visited Aug. 30, 2019) ("Yes, we do. We create partnerships between you, our patients, and the companies that are developing products to help you. To do that, we take the information you entrust to us and sell it to the companies that can use that data to improve or understand products or the disease market."); *Privacy Policy*, PATIENTSLIKEME, https://www.patientslikeme.com/about/privacy (last visited Aug. 30, 2019) [hereinafter *PatientsLikeMe Privacy Policy*] ("PatientsLikeMe frequently partners with other institutions to conduct research. These Partners include, but are not limited to: universities, pharmaceutical companies, hospital systems, insurance companies, and regulatory bodies . . . .").

66 *Under Armour Inc*, REUTERS, https://www.reuters.com/finance/stocks/company-profile/UA (last visited Aug. 30, 2019).

67 *See Under Armour Headquarters and Office Locations*, CRAFT, https://craft.co/under-armour/locations (last visited Sept. 16, 2019).

68 *The UA Story*, M ADVANTAGE (last visited Oct. 13, 2019), https://static.umterps.com/custompages/maryland_advantage/phone/the-ua-story.html.

69 *See Under Armour*, GOOGLE, https://play.google.com/store/apps/developer?id=under+Armour&hl=EN_US (last visited Aug. 30, 2019) (showing that Under Armour owns and operates a number of mobile apps, including Under Armour, Under Armour Record, and UA Play); *Under Armour Privacy Policy*, UNDER ARMOUR (Apr. 20, 2018), https:/

well as identifiers such as names, usernames, hashed passwords, physical addresses, email addresses, dates of birth, payment card information, and approximate or precise locations.[70] Available in the Apple App Store for iOS and on Google Play for Android,[71] MyFitnessPal states in its privacy policy that it uses entered data for research purposes and that it discloses the data for advertising, marketing, and other purposes.[72]

On March 25, 2018, Under Armour learned that an unauthorized third party accessed MyFitnessPal user data, including usernames, email addresses, and hashed passwords.[73] Four days later, on March 29, Under Armour publicly announced that hackers stole the data of more than 150 million MyFitnessPal users.[74] The following day, March 30, Under Armour notified these users, including this author, of the data breach through a formal process called breach notification.[75] In the breach notification email, Under Armour provided information regarding how MyFitnessPal users could protect themselves, including by changing their passwords, reviewing their accounts for suspicious activity, being cautious of unsolicited communications, and avoiding clicking on links or downloading attachments from suspicious emails.[76] Although MyFitnessPal clearly followed some type of breach notification policy, it is unclear whether MyFitnessPal had implemented privacy standards and security safeguards that could have prevented the breach in the first place.

II. Federal and International Standards

A variety of federal and international legal authorities have been interpreted to impose privacy, security, and breach notification obligations on individuals and institutions that collect, use, or disclose health data in certain

/account.underarmour.com/en-us/privacy (showing that Under Armour additionally operates MyFitnessPal and other fitness apps).

70 *See Under Armour Privacy Policy*, *supra* note 69.

71 *MyFitnessPal*, Apple, https://apps.apple.com/us/app/myfitnesspal/id341232718 (last visited Aug. 30, 2019); *MyFitnessPal*, Google, https://play.google.com/store/apps/details?id=com.myfitnesspal.android&hl=EN_US (last visited Aug. 30, 2019).

72 *See Under Armour Privacy Policy*, *supra* note 69.

73 *See* E-mail from Paul Fipps, Chief Digital Officer, MyFitnessPal, to Stacey Tovino (Mar. 30, 2018, 5:52 PM) (on file with author) [hereinafter MyFitnessPal Data Breach Notification] (notifying the author that the privacy and security of her own MyFitnessPal data had been breached).

74 *See, e.g.*, Sara Germano & Maria Armental, *Under Armour Discloses Breach Affecting 150 Million MyFitnessPal App Users*, Wall St. J. (Mar. 29, 2018), https://www.wsj.com/articles/under-armour-discloses-breach-affecting-150-million-myfitnesspal-app-users-1522362412 (reporting the data breach); Hamza Shaban, *Under Armour Announces Data Breach, Affecting 150 Million MyFitnessPal App Accounts*, Wash. Post (Mar. 29, 2018), https://www.washingtonpost.com/news/the-switch/wp/2018/03/29/under-armour-announces-data-breach-affecting-150-million-myfitnesspal-app-accounts/?noredirect=ON (same).

75 *See* MyFitnessPal Data Breach Notification, *supra* note 73.

76 *Id.*

contexts.[77] Under federal consumer law, for example, when a company tells a consumer that the company will safeguard the consumer's health data but fails to do so, the Federal Trade Commission (FTC) can take enforcement action, forcing the company to keep its promise.[78] Although the FTC Act does not contain particular data privacy and security standards, section 5 of the FTC Act does prohibit "unfair or deceptive acts or practices."[79] The FTC has relied on this broad language in more than one hundred enforcement actions involving unfair data collection practices as well as broken privacy and security promises.[80] Through these actions, the FTC hopes to protect consumers against information-related injuries, including deception injuries, financial injuries, health and safety injuries, intrusion injuries, and reputational injuries.[81]

In *FTC v. Wyndham*, for example, Wyndham Hotels and Resorts agreed to settle FTC charges that the company's faulty data security practices unfairly exposed the payment-card information of hundreds of thousands of

77 *See, e.g.*, 15 U.S.C. §§ 6801–09, 6821–27 (2012) (requiring financial institutions to provide notice to customers of privacy policies and practices, regulating financial institutions' disclosure of nonpublic personal information, and requiring financial institutions to develop an information security plan); Data Protection Act 2018, c.12 (UK) (regulating the processing of personal data); Privacy of Consumer Financial Information, 16 C.F.R. pt. 313 (2019) (federal regulations implementing the Gramm-Leach-Bliley Act); Cameron Abbot, *Facebook Fined £500,000 Over Cambridge Analytica Scandal*, NAT'L L. REV. (July 13, 2018), https://www.natlawreview.com/article/facebook-fined-500000-over-cambridge-analytica-scandal (reporting that the UK Information Commissioner's Office fined Facebook £500,000 for violating UK's Data Protection Act of 1998 following Facebook's failure to protect user data and Facebook's lack of transparency regarding its handling of user data).

78 *See, e.g.*, *Privacy and Security Enforcement*, FED. TRADE COMM'N, https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/privacy-security-enforcement (last visited Sept. 24, 2019) ("The FTC has brought legal actions against organizations that have violated consumers' privacy rights, or misled them by failing to maintain security for sensitive consumer information. In many of these cases, the FTC has charged the defendants with violating Section 5 of the FTC Act, which bars unfair and deceptive acts and practices in or affecting commerce.").

79 15 U.S.C. § 45(a)(1) (2012) ("Unfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce, are hereby declared unlawful.").

80 *See generally* Alexander E. Reicher & Yan Fang, *FTC Privacy and Data Security Enforcement and Guidance Under Section 5*, J. ANTITRUST, UCL & PRIVACY SEC. ST. B. CAL., Fall 2016, at 89, 89 (providing outstanding guidance regarding the contours of the FTC's privacy and security enforcement under section 5 of the FTC Act, and stating that the FTC has brought more than one hundred privacy and security cases using Section 5 of the FTC Act); Maureen K. Ohlhausen, Chairman, Fed. Trade Comm'n, Speech at Federal Communications Bar Association Luncheon: Painting the Privacy Landscape: Informational Injury in FTC Privacy and Data Security Cases 1–2 (Sept. 19, 2017), https://www.ftc.gov/system/files/documents/public_statements/1255113/privacy_speech_mkohlhausen.pdf (noting that the FTC has brought "more than 500 privacy and data security cases, both online and off" under a number of different statutes, including the Gramm-Leach-Bliley Act and the Children's Online Privacy Protection Act).

81 *See* Ohlhausen, *supra* note 80, at 1, 3–9 (summarizing and providing examples of these five types of consumer information injuries).

consumers to hackers in three separate data breaches, thus exposing Wyndham guests to financial injuries.[82] As part of its December 2015 settlement, Wyndham agreed to establish a comprehensive information-security program, conduct annual information-security audits, and prevent future hackers from stealing consumer data, among other measures.[83]

Although the Wyndham case involved stolen, payment-card data, other FTC cases have involved stolen health data. In an August 2013 complaint against Atlanta-based LabMD, for example, the FTC alleged that the clinical laboratory testing company failed to reasonably protect the security of its patients' identifiable health data and that this failure constituted an unfair practice affecting consumers in violation of section 5 of the FTC Act.[84] The FTC specifically alleged that LabMD failed to protect the names, social security numbers, dates of birth, health insurance policy numbers, and standardized health procedure codes of 9300 patients.[85]

In its press release announcing the complaint against LabMD, the FTC stated that it was "committed to ensuring that firms who collect . . . data [take] reasonable and appropriate security measures to prevent it from falling into the hands of identity thieves and other unauthorized users."[86] In a separate press release, the FTC explained: "[A] company's data security measures must be reasonable and appropriate in light of the sensitivity and volume of consumer information it holds, the size and complexity of its business, and the cost of available tools to improve security and reduce vulnerabilities."[87] It is clear, then, that under federal consumer law, mobile health apps must implement reasonable and appropriate security measures

82 *See* Press Release, Fed. Trade Comm'n, Wyndham Settles FTC Charges It Unfairly Placed Consumers' Payment Card Information at Risk (Dec. 9, 2015) [hereinafter FTC/Wyndham Press Release], https://www.ftc.gov/news-events/press-releases/2015/12/wyndham-settles-ftc-charges-it-unfairly-placed-consumers-payment (announcing the settlement); *Wyndham Worldwide Issues Statement on FTC Settlement*, PR NEWSWIRE (Dec. 9, 2015), https://www.prnewswire.com/news-releases/wyndham-worldwide-issues-statement-on-ftc-settlement-300190509.html (same). *See generally* Jennifer K. Wagner, Assoc. Dir. of Bioethics Research, Geisinger, FTC Regulation of Mobile Health Apps (Apr. 24, 2018) (unpublished PowerPoint presentation) (on file with author) (providing an outstanding overview of FTC regulation of mobile health apps).

83 *See* FTC/Wyndham Press Release, *supra* note 82.

84 Complaint at 3, ¶ 10, *In re* LabMD, Inc., FTC File No. 102-3099, Docket No. 9357 (Aug. 28, 2013) [hereinafter LabMD Complaint], https://www.ftc.gov/sites/default/files/documents/cases/2013/08/130829labmdpart3.pdf; Press Release, Fed. Trade Comm'n, FTC Files Complaint Against LabMD for Failing to Protect Consumers' Privacy (Aug. 29, 2013) [hereinafter FTC/LabMD Press Release], https://www.ftc.gov/news-events/press-releases/2013/08/ftc-files-complaint-against-labmd-failing-protect-consumers.

85 *See* LabMD Complaint, *supra* note 84, at 4–5; FTC/LabMD Press Release, *supra* note 84.

86 FTC/LabMD Press Release, *supra* note 84.

87 FED. TRADE COMM'N, COMMISSION STATEMENT MARKING THE FTC'S 50TH DATA SECURITY SETTLEMENT 1 (2014), https://www.ftc.gov/system/files/documents/cases/140131gmrstatement.pdf.

and not make statements regarding such measures that are false, misleading, or deceptive.[88]

Section 5 of the FTC Act is not the only legal authority to impose data privacy and security obligations on data collectors in certain contexts. The current version of the Federal Common Rule, for example, contains a regulation designed in part to protect research-participant privacy and research-data confidentiality.[89] As background, the Common Rule regulates nonexempt, human-subjects research that receives federal financial support from a signatory federal agency[90] and research conducted in contemplation of a submission to the Food and Drug Administration (FDA) for approval.[91] Although many research protocols are subject to the Common Rule due to federal funding, an FDA submission, a state law that requires compliance with the Common Rule, or a researcher employment contract or affiliation agreement requiring compliance with the Common Rule, some mobile-app-mediated research studies remain free of Common Rule regulation.[92]

For research that is subject to the Common Rule, the overarching goal of the Common Rule is to protect the health, safety, and welfare of research participants. Protecting the privacy of research participants and the confidentiality of their research data is one part of that larger goal.[93] Indeed, institutional review boards (IRBs) that review research to ensure compliance with the Common Rule must find "adequate provisions to protect the privacy

88 Although neither Wyndham nor LabMD were collecting health data through a mobile health app, the FTC has taken several enforcement actions against mobile apps in the context of deceptive claims and broken promises. *See* Complaint for Permanent Injunction and Other Equitable Relief at 4, FTC v. Pact, Inc., No. 2:17-cv-01429 (W.D. Wash. Sept. 21, 2017), https://www.ftc.gov/system/files/documents/cases/1523010 pactcomplaint.pdf (noting that the defendant mobile app "continued to charge (rather than pay) many consumers who have completed their pacts and bill consumers who have attempted to cancel the service, despite continued promises to the contrary"); *Mobile Technology Issues*, FED. TRADE COMM'N, https://www.ftc.gov/news-events/media-resources/mobile-technology (last visited Sept. 16, 2019) (linking to a number of press releases announcing enforcement actions involving mobile apps).

89 *See* text accompanying *infra* note 94.

90 *See, e.g.*, Federal Policy for the Protection of Human Subjects: Six Month Delay of the General Compliance Date of Revisions While Allowing the Use of Three Burden-Reducing Provisions During the Delay Period, 83 Fed. Reg. 28,497 (June 19, 2018) (to be codified in scattered titles of the Code of Federal Regulations) [hereinafter Final Common Rule Amendments] (listing the agencies that have signed on to the Common Rule).

91 *See generally* 45 C.F.R. § 46.101–.124 (2018) (codifying HHS's Common Rule); Final Common Rule Amendments, *supra* note 90, at 28,518 (showing changes to HHS's Common Rule with which compliance is required by Jan. 21, 2019); Mark A. Rothstein, *Research Privacy Under HIPAA and the Common Rule*, 33 J.L. MED. & ETHICS 154, 155 (2005) (explaining the application of the Common Rule).

92 *See* Michelle N. Meyer, Assistant Professor, The Common Rule and Research with Mobile Devices (Apr. 24, 2018) (unpublished PowerPoint presentation), https://louisville.edu/mobileelsi/wgm-2-thought-leader-input-and-regulatory-framework/presentation-by-michelle-meyer/ (explaining in detail when research is regulated by the Common Rule).

93 *See* Rothstein, *supra* note 91, at 155.

of subjects and to maintain the confidentiality of data," when appropriate, in order for the research to proceed.[94] Although IRBs have the primary responsibility for ensuring researcher compliance with the Common Rule,[95] the Federal Office for Human Research Protections (OHRP) within HHS maintains regulatory oversight as well.[96]

In addition to federal authorities such as section 5 of the FTC Act and the Common Rule, several state constitutions contain a right to privacy that has been interpreted to protect individually identifiable health information.[97] Florida's constitution, for example, provides that "[e]very natural person has the right to be let alone and free from governmental intrusion into the person's private life except as otherwise provided herein."[98] Long understood to protect an individual's right to privacy vis-à-vis governmental intrusions, scholars have pushed to extend Florida's constitutional right to privacy to nongovernmental intrusions as well, although these efforts have, to date, been unsuccessful.[99] Other state constitutions, including those of Alaska, Arizona, California, Hawaii, Illinois, Louisiana, Montana, South Carolina, and Washington, also establish rights to privacy applicable to health information.[100]

Section 5 of the FTC Act, the Federal Common Rule, and the state constitutions listed above are illustrative, but not exhaustive, examples of legal authorities that have been interpreted to require certain health data holders in certain contexts to maintain data privacy and security.[101] Note, however, that not one of these legal authorities sets forth particular privacy and security standards. Indeed, section 5 of the FTC Act does not mention the words

94 *See* 45 C.F.R. § 46.111(a)(7) (2018).

95 Rothstein, *supra* note 91, at 155.

96 *See Office for Human Research Protections*, U.S. DEP'T HEALTH & HUMAN SERVS., https://www.hhs.gov/ohrp/ (last visited Sept. 16, 2019) ("[OHRP] provides leadership in the protection of the rights, welfare, and wellbeing of human subjects involved in research conducted or supported by the [HHS]. . . . OHRP provides clarification and guidance, develops educational programs and materials, maintains regulatory oversight, and provides advice on ethical and regulatory issues in biomedical and behavioral research.").

97 *See, e.g.*, Catherine Louisa Glenn, Note, *Protecting Health Information Privacy: The Case for Self-Regulation of Electronically Held Medical Records*, 53 VAND. L. REV. 1605, 1609 n.25 (2000) (referencing the state constitutions of Alaska, Arizona, California, Florida, Hawaii, Illinois, Louisiana, Montana, South Carolina, and Washington as establishing rights to privacy applicable to health information).

98 FLA. CONST. art. I, § 23.

99 *See* Ben F. Overton & Katherine E. Giddings, *The Right of Privacy in Florida in the Age of Technology and the Twenty-First Century: A Need for Protection from Private and Commercial Intrusion*, 25 FLA. ST. U. L. REV. 25, 53–55 (1997) (recommending that Florida's constitution be amended to protect against nongovernmental intrusions as well as governmental intrusions).

100 *See* Glenn, *supra* note 97, at 1609 n.25.

101 *See, e.g.*, Stacey A. Tovino, *Florida Law, Mobile Research Applications, and the Right to Privacy*, 43 NOVA L. REV. 353 (2019) (identifying additional sources of protection under Florida law).

privacy and security at all[102] and the Common Rule contains only one IRB review criterion (among seven) referencing privacy and confidentiality.[103] Even California's constitution, recognized as one of the broadest in the country, only provides: "All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy."[104]

Other domestic and international laws do, however, set forth specific privacy, security, and breach notification standards that may be used to guide the conduct of mobile-app-mediated health research by independent researchers, citizen scientists, and patient researchers as well as other health data collectors and processors. In the United States, the HIPAA Rules establish detailed privacy, security, and breach notification standards[105] for cov-

102 *See* 15 U.S.C. § 45(a)(1) (2012) ("Unfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce, are hereby declared unlawful."). The FTC has published a variety of privacy and security suggestions, recommendations, guidelines, and best practices (collectively, best practices); however, these best practices are not codified or promulgated in statutes or regulations. *See, e.g.*, FED. TRADE COMM'N, MARKETING YOUR MOBILE APP: GET IT RIGHT FROM THE START 1, 2–5 (2013), https://www.ftc.gov/system/files/documents/plain-language/pdf-0140_marketing-your-mobile-app.pdf (providing general guidelines for consideration by mobile-app developers, including guidelines such as "[b]uild privacy considerations in from the start," "[b]e transparent about your data practices," "[h]onor your privacy promises," "[p]rotect kids' privacy," "[c]ollect sensitive information only with consent," and "[k]eep user data secure"); FED. TRADE COMM'N, MOBILE PRIVACY DISCLOSURES: BUILDING TRUST THROUGH TRANSPARENCY, at i, 1–29 (2013), https://www.ftc.gov/sites/default/files/documents/reports/mobile-privacy-disclosures-building-trust-through-transparency-federal-trade-commission-staff-report/130201mobileprivacyreport.pdf (offering several suggestions for "major participants in the mobile ecosystem" as they "work to improve mobile privacy disclosures"); FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE 22–71 (2012) (setting forth best practices in the areas of privacy by design, simplified consumer choice, and transparency); *Mobile Health App Developers: FTC Best Practices*, FED. TRADE COMM'N (Apr. 2016), https://www.ftc.gov/tips-advice/business-center/guidance/mobile-health-app-developers-ftc-best-practices (providing best privacy and security practices for mobile health app developers); *Privacy and Security*, FED. TRADE COMM'N, https://www.ftc.gov/tips-advice/business-center/privacy-and-security (last visited Sept. 16, 2019) (providing summaries of major pieces of federal legislation relating to privacy and security); Ohlhausen, *supra* note 80 (addressing consumer injury in the FTC's privacy and security cases and identifying and warning against five types of consumer informational injuries).

103 *See* 45 C.F.R. § 46.111(a)(7) (2018) (setting forth seven IRB review criteria; the seventh criterion provides: "When appropriate, there are adequate provisions to protect the privacy of subjects and to maintain the confidentiality of data.").

104 CAL. CONST. art. I, § 1 (amended 1974).

105 *See, e.g.*, John Soma et al., *Chasing the Clouds Without Getting Drenched: A Call for Fair Practices in Cloud Computing Services*, 16 J. TECH. L. & POL'Y 193, 217 (2011) (referencing HIPAA as an industry-specific standard); Grace Fleming, Note, *HIPAA-Cratic or HIPAA-Critical: U.S. Privacy Protections Should Be Guaranteed by Covered Entities Working Abroad*, 98 MINN. L. REV. 2375, 2379 (2014) (noting that HIPAA was enacted, in part, in response to the need for an industry standard in the context of electronic health records).

ered entities and business associates that use or disclose a subset of individually identifiable health information known as protected health information (PHI).[106] In the European Union, the General Data Protection Regulation (GDPR) is quickly becoming known as the global standard in all industries (not just the healthcare industry) for individuals and institutions that control and process all types of personal data, including health data.[107] The remainder of this Part reviews the application of the HIPAA Rules and the GDPR as well as the specific privacy, security, and breach notification standards set forth therein. The purpose of this review is to highlight core privacy, security, and breach notification principles that could serve as a guide for mobile-app-mediated research conducted by independent scientists and other big data processors while also noting the limitations of these regulations.

A. Application of the HIPAA Rules and the GDPR

The HIPAA Rules, including the HIPAA Privacy, Security, and Breach Notification Rules,[108] regulate covered entities[109] and business associates.[110] Again, covered entities include health plans,[111] healthcare clearinghouses,[112] and those healthcare providers that transmit health information in electronic form in connection with certain standard transactions including the health claim transaction.[113] A business associate is a person or organization that provides certain services to a covered entity, other than in the capacity of a workforce member of the covered entity, who needs access to PHI to perform the service.[114] With four, rarely implicated exceptions, PHI is indi-

106 45 C.F.R. § 160.103 (2018) (defining protected health information).

107 *See, e.g.*, Sheera Frenkel, *Tech Giants Brace for Europe's New Data Privacy Rules*, N.Y. TIMES (Jan. 28, 2018), https://www.nytimes.com/2018/01/28/technology/europe-data-privacy-rules.html (reporting that Europe has set the "regulatory standard" in terms of data privacy with the GDPR); *id.* (quoting Julie Brill, corporate vice president and deputy general counsel at Microsoft, as stating that Microsoft "embrace[s] [the] G.D.P.R. because it sets a strong standard for privacy and data protection rights"); Mark Scott & Laurens Cerulus, *Europe's New Data Protection Rules Export Privacy Standards Worldwide*, POLITICO (Jan. 31, 2018), https://www.politico.eu/article/europe-data-protection-privacy-standards-gdpr-general-protection-data-regulation/ ("Since the mid-1990s, EU policymakers have rolled out a series of data protection rules that quickly became the de facto global standards for most countries except for a few holdouts."); *id.* (quoting Vera Jourová, the European commissioner for justice, as stating that the European Union "want[s] to set the global standard" with the GDPR).

108 *See* sources cited *supra* note 10.

109 45 C.F.R. § 160.103 (2018) (defining covered entity); *id.* § 160.102(a) (applying the HIPAA Rules to covered entities).

110 *Id.* § 160.103 (defining business associate); *id.* § 160.102(b) (applying the HIPAA Rules to business associates).

111 *Id.* § 160.103 (defining health plan).

112 *Id.* (defining healthcare clearinghouse).

113 *Id.* (defining covered entity).

114 *Id.* (defining business associate).

vidually identifiable health information.[115] Health information that has been properly deidentified, however, is not regulated by the HIPAA Rules.[116] One permissible method of deidentifying information involves the removal of eighteen different identifiers from the data including, but not limited to, names, all geographic subdivisions smaller than a state, all elements of dates except for year for individuals eighty-nine years of age and younger, full-face photographic images and comparable images, and any other unique identifying number, characteristic, or code.[117]

Neither ActiveDay, PatientsLikeMe, nor MyFitnessPal is owned or operated by a covered healthcare provider, health plan, healthcare clearinghouse, or business associate thereof. Neither ActiveDay, PatientsLikeMe, nor MyFitnessPal performs covered provider, plan, clearinghouse, or business associate functions. Therefore, the HIPAA Rules generally will not regulate these mobile apps.[118] That is, the United States' primary privacy, security, and

115 *Id.* (defining "individually identifiable health information" as a subset of health information that is "created or received by a health care provider, health plan, employer, or health care clearinghouse" and that "[r]elates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual"); *id.* (listing the four exclusions from the definition of PHI).

116 *Id.* § 164.514(a) ("Health information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual is not individually identifiable health information."); *id.* § 164.514(b)(1)–(2) (setting forth two methods for health information to be considered deidentified).

117 *Id.* § 164.514(b)(2) (listing the eighteen identifiers that must be removed from protected health information for the information to be considered deidentified).

118 To the extent the companies that own and operate these mobile apps offer health insurance to their employees through a group health plan, the HIPAA Rules will regulate the group health plan if such plan has fifty or more participants or is administered by a third-party administrator (TPA). *See id.* § 160.103 (defining covered entity to include health plans); *id.* (defining health plan to include group health plan); *id.* (defining group health plan to include an employee welfare benefit plan with fifty or more participants as well as those administered by a TPA). Tidyware, which operates ActiveDay, appears to be a small company that may or may not offer health insurance to its employees; if it does offer health insurance to its employees through a group health plan, there may not be fifty or more participants in that health plan. *See Tidyware LLC*, MANTA, https://www.manta.com/c/mb42sxd/tidyware-llc (last visited Aug. 28, 2019) ("Tidyware LLC is a privately held company in Bellevue, WA[,] . . . [that] was established in 2012 and incorporated in Washington. Current estimates show this company has an annual revenue of [$]204,157 and employs a staff of approximately 3."). On the other hand, Under Armour is a large company that offers three different types of health plans to thousands of employees. *See Benefits at Under Armour*, UNDER ARMOUR, https://tbcdn.talentbrew.com/company/7686/v1_0/doc/UA_RecruitBenefitsOverview_121918_4.pdf (last visited June 25, 2018) (describing the health insurance benefits available to full-time Under Armour employees). Under Armour thus has a group health plan that is regulated by the HIPAA Rules. To the extent Under Armour has taken advantage of HIPAA's hybrid-entity rules, designating its group health plan as a covered healthcare component and MyFitnessPal as a nonhealthcare component, the HIPAA Rules do not apply to MyFitnessPal. *See infra* note 121 (discussing HIPAA's hybrid-entity rules).

breach notification standards applicable to the healthcare industry simply do not apply, even though ActiveDay, PatientsLikeMe, and MyFitnessPal collect, use, and disclose a fair amount of health data. In this sense, the HIPAA Rules have not kept pace with the individuals and institutions that are collecting, using, and disclosing health data.

Kinsey Reporter is a joint project of the Kinsey Institute for Research in Sex, Gender, and Reproduction (KI) and the Center for Complex Networks and Systems Research (CNetS), both at Indiana University (IU), Bloomington.[119] IU does perform some HIPAA-covered functions through its student health center, its medical and other health professional schools, and its employee group health plan.[120] However, IU has taken advantage of HIPAA's hybrid-entity rules to exclude KI and CNetS from its designated healthcare components.[121] The result is that the HIPAA Rules do not apply to the projects of KI and CNetS, including Kinsey Reporter. Stated another way, the data Kinsey Reporter collects related to sexual health and other intimate behavior is not protected by the HIPAA Rules.

Assuming for the moment that the HIPAA Rules did apply to Kinsey Reporter, ActiveDay, PatientsLikeMe, and MyFitnessPal, all four apps collect health information that is not deidentified in accordance with the HIPAA Privacy Rule. For example, Kinsey Reporter collects sexual and reproductive health information (e.g., missed menses associated with the ingestion of hormonal birth control) combined with the city, state, and country (e.g., "Seminole, FL, US") of the reporting citizen sex scientist.[122] Because the HIPAA Privacy Rule requires cities and other geographic designations smaller than a state to be removed in order for health information to be deidentified, the data collected by Kinsey Reporter would not be considered deidentified.[123]

Similarly, ActiveDay and FallSafety Pro collect data regarding current physical status and provision of care by a first responder combined with the precise geolocation of the citizen scientist who fell, exercised, or otherwise

119 *See Kinsey Reporter Privacy Policy*, *supra* note 40.

120 *See* IND. UNIV., HIPAA-A03, DESIGNATION OF INDIANA UNIVERSITY AS A HYBRID ENTITY, at attachment A (2014) (listing the Indiana University Health Center; the Indiana University Counseling and Psychological Services; the Indiana University Schools of Arts & Science, Medicine, Dentistry, and Optometry; and the Indiana University health plans as HIPAA-covered health care components).

121 *See* 45 C.F.R. § 164.103 (defining, for purposes of the HIPAA Rules, a hybrid entity as a single legal entity whose business activities include both covered and noncovered functions); *id.* § 164.105(c)(1) (requiring a covered entity that wishes to take advantage of HIPAA's hybrid-entity rules to designate itself as a hybrid entity and to document that designation); *id.* § 164.105(a)(1) (stating that the HIPAA Rules only apply to the designated health care components of a hybrid entity); IND. UNIV., *supra* note 120 (designating IU as a hybrid entity); *id.* at attachment A (listing IU's HIPAA-covered health care components and not including KI within that list).

122 *See supra* notes 38–41 and accompanying text (identifying the data elements gathered by Kinsey Reporter from its citizen sex scientists).

123 45 C.F.R. § 164.514(b)(2)(i) ("The following identifiers of the individual . . . [must be] removed: . . . [a]ll geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes . . . .").

moved.[124] Again, the HIPAA Privacy Rule requires all geographic subdivisions smaller than a state to be removed in order for health information to be deidentified. Thus, the data collected by ActiveDay and FallSafety Pro would not meet the HIPAA Privacy Rule's deidentification standard.

Likewise, PatientsLikeMe collects a significant amount of data regarding individuals' physical and mental health (e.g., colon cancer, genital herpes, HIV, obesity, paranoid schizophrenia, alcohol-use disorder, and drug-use disorder) combined with a number of identifiers (e.g., names, user names, full facial photographs, and ages).[125] Like the data collected by Kinsey Reporter and ActiveDay, the data collected by PatientsLikeMe would not meet the HIPAA Privacy Rule's deidentification standard if the HIPAA Rules applied.

Finally, MyFitnessPal collects a fair amount of physical health information, including body weight and nutritional information, combined with identifiers including names, usernames, physical addresses, email addresses, dates of birth, and approximate or precise locations when exercising or inputting data.[126] The data collected by MyFitnessPal would not be considered deidentified either. In large summary, the HIPAA Rules are too limited in application. That is, they do not protect the data collected by four illustrative mobile research apps even though the data collected by the apps relate to health and are clearly identifiable or could lead to the identification of the data subject.

Although the HIPAA Rules were designed to regulate health industry participants—including healthcare providers, healthcare clearinghouses, health plans, and business associates thereof—the GDPR was designed to protect personal data regardless of the industry or context in which the data was generated or is maintained. In particular, the GDPR regulates (1) personal data controllers and processors established in the European Union, regardless of whether the data processing takes place inside or outside the European Union; (2) the processing of personal data of data subjects who are in the EU by a controller or processor not established in the EU if the data processing relates to the offering of goods or services to data subjects in the European Union or the monitoring of behavior in the European Union by data subjects; and (3) the processing of personal data by a controller not established in the European Union but in a place where a member state's law applies by virtue of public international law.[127]

---

124 *FallSafety Privacy Policy*, *supra* note 54 ("FallSafety may use third party services that may collect user information. These services include . . . geolocation services . . . . These services may collect information sent by your browser such as cookies or your IP request.").

125 *See* text accompanying *supra* notes 63–65 (discussing the data collected by PatientsLikeMe).

126 *See* text accompanying *supra* note 69–70 (discussing the data collected by MyFitnessPal).

127 Commission Regulation (EU) 2016/679, 2016 O.J. (L 119) (EU), art. 3(1)–(3) [hereinafter GDPR]; European Data Prot. Bd., Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) (Nov. 16, 2018), https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_3_2018_territorial_scope_en.pdf (explaining—and illustrating with examples—the territorial scope of the GDPR).

The GDPR defines a data controller as any "natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data."[128] The GDPR's regulation of natural persons will become important in Part III, where the author will show that some states currently regulate only government agencies or similar institutions, but not natural persons. The author will argue that these statutes should be expanded to regulate natural persons as well.

The GDPR also defines a data processor as any "natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller."[129] Processing means "any operation or set of operations which is performed on personal data . . . [including the] collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, . . . combination, restriction, erasure, or destruction [of data]."[130] Personal data means "any information relating to an identified or identifiable natural person."[131] An identifiable natural person is a person "who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."[132]

All four mobile apps—Kinsey Reporter (through IU's Kinsey Institute and CNetS), ActiveDay (through Tidyware), PatientsLikeMe, and MyFitnessPal (through Under Armour)—would meet the GDPR's definition of a data controller. That is, all four companies and/or apps involve natural or legal persons who are collecting, using, and disclosing personal data relating to physical or physiological health. In the cases of PatientsLikeMe and MyFitnessPal, the personal data collected is clearly identifiable due to the apps' collection of names, online identifiers, and other identifiers. In the cases of Kinsey Reporter and ActiveDay, it is not clear whether the personal data is identifiable. Kinsey Reporter only collects the general (city) location of the reporting citizen sex scientist. ActiveDay does, however, collect the precise geolocation of the reporting citizen scientist.

Because PatientsLikeMe and MyFitnessPal monitor the behavior of data subjects in the European Union, the data collected by these two apps are clearly protected by the GDPR.[133] To the extent the data collected by Kinsey Reporter meets the GDPR's identifiability standard, the data collected by Kin-

128 GDPR, *supra* note 127, art. 4(7).

129 *Id.* art. 4(8).

130 *Id.* art. 4(2).

131 *Id.* art. 4(1).

132 *Id.*

133 *See PatientsLikeMe Privacy Policy*, *supra* note 65; *Under Armour Privacy Policy*, *supra* note 69.

sey Reporter also may be regulated by the GDPR.[134] To the extent the data collected by ActiveDay meets the GDPR's identifiability standard and to the extent that ActiveDay monitors the behavior of data subjects in the European Union (which the author was unable to discover), then ActiveDay also may be regulated by the GDPR. In summary, an EU cross-industry regulation, but not the HIPAA Rules, protects the health data collected by at least two of the illustrative, U.S.-based, mobile research apps discussed in this Article.

Assuming for the moment that the HIPAA Rules do protect the data collected by Kinsey Reporter, ActiveDay, PatientsLikeMe, and MyFitnessPal, either through an amendment to the definition of covered entity or through a new statute or regulation containing similar substantive requirements, are there particular provisions within the HIPAA Rules (or the GDPR) that are important to apply to mobile-app-mediated health research? A brief review of the substance of each of the HIPAA Rules and the GDPR is necessary before proceeding.

B. Privacy

1. The Use and Disclosure Requirements

The HIPAA Privacy Rule contains three groups of subregulations, including the "use and disclosure" requirements,[135] the individual rights,[136] and the administrative requirements.[137] In terms of its use and disclosure requirements, the HIPAA Privacy Rule requires covered entities and business associates to adhere to one of three different requirements depending on the purpose of the information use or disclosure.[138] The first use and disclosure requirement allows covered entities and business associates to use and disclose PHI with no prior permission from the individual who is the subject of the PHI—but only in certain situations. That is, covered entities may freely use and disclose PHI without any form of prior permission in order to carry out certain treatment, payment, and healthcare operations[139] activities (collectively, TPO activities),[140] as well as certain public-benefit activities.[141]

134 *See Explore: Top Surveys in IT*, KINSEY REPORTER, https://kinseyreporter.org/#/explore?country=1 (showing that several citizen sex scientists located in Italy have used Kinsey Reporter to report female hormonal birth control use and effects).

135 45 C.F.R. §§ 164.502–.514 (2018).

136 *Id.* §§ 164.520–.528.

137 *Id.* § 164.530.

138 *Id.* §§ 164.502–.514 (setting forth the use and disclosure requirements applicable to covered entities and business associates). In a number of prior articles, this author carefully reviewed the history, application, and general framework of the HIPAA Privacy Rule. *See, e.g.*, Tovino, *A Timely Right to Privacy*, *supra* note 22, at 1367–74 (detailing the history of the HIPAA Privacy Rule with a focus on civil enforcement). With updates and technical changes, the brief summary of the HIPAA Privacy Rule set forth in Section II.B of this Article is taken with the permission of the author from these prior publications.

139 45 C.F.R. § 164.501 (defining treatment, payment, and health care operations).

140 *See id.* § 164.506(c)(1) (permitting a covered entity to use or disclose PHI for its own treatment, payment, or health care operations); *id.* § 164.506(c)(2)–(4) (permitting a

Assuming that the HIPAA Rules were extended to the four mobile research apps discussed in this Article, the treatment and payment provisions in the first use and disclosure requirement would have little application or relevance. In general, independent scientists who own, operate, or use mobile research apps are not themselves providing healthcare, submitting claims to insurers for such healthcare, paying claims submitted by participating providers, engaging in most healthcare operations activities, or participating in public-benefit activities. In summary, and to the extent the HIPAA Privacy Rule was used as a guide for the future regulation of mobile-app-mediated research conducted by independent scientists, it would not be as important to have a TPO provision or a complete public-benefits provision allowing the unauthorized use and disclosure of research participants' health data. Stated another way, the HIPAA Privacy Rule's concentrated focus on treatment, payment, operations, and other traditional activities engaged in by healthcare providers and health plans is outdated given the growth in non-covered-entity collection, use, and disclosure of health data.

Under the HIPAA Privacy Rule's second use and disclosure requirement, a covered entity or business associate may use and disclose an individual's PHI for certain activities, but only if the individual is informed (orally or in writing) in advance of the use or disclosure and is given the (oral or written) opportunity to agree to, prohibit, or restrict the use or disclosure.[142] The certain activities captured by this provision include, but are not limited to, disclosures of PHI (1) from a healthcare provider's facility directory; (2) to a person who is involved in an individual's care or payment for care; and (3) for certain notification purposes, such as when an attending physician or a hospital social worker notifies a partner or spouse of a patient's death.[143]

Like the first use and disclosure requirement, this second use and disclosure requirement also has low application in the instant context. Independent scientists tend not to affiliate with hospitals and other healthcare facilities that have patient directories. As nonhealthcare providers, they also do not provide patient care or accept payment for care, and thus do not have a need to disclose PHI to persons involved in patient care or payment for care. Therefore, and to the extent the HIPAA Privacy Rule was used as some type of reference guide for the future regulation of independent, mobile-app-based research, it would not be important to have an oral agreement provision. It would not be practical either, given the remote nature of mobile-app-mediated research.

---

covered entity to disclose PHI to certain recipients for the recipients' treatment, payment, or health care operations activities, respectively).

141 Covered entities may use and disclose PHI for twelve different public-policy activities without the prior written authorization of the individual who is the subject of the information. *See id.* § 164.512(a)–(l).

142 *See id.* § 164.510 (titled "Uses and disclosures requiring an opportunity for the individual to agree or object").

143 *See id.* § 164.510(a), (b)(1)(i)–(ii).

The HIPAA Privacy Rule's third use and disclosure requirement—a default rule—requires covered entities and business associates to obtain the prior written authorization of the individual who is the subject of the PHI before using or disclosing the individual's PHI in any situation that does not fit within the first two rules.[144] If the HIPAA Privacy Rule was used as some type of roadmap for the future regulation of independent, mobile-app-based research, this rule would be relevant. That is, mobile health research apps collect, use, and/or disclose PHI for a purpose—research—that typically does not fit within the first two rules.[145] Although much has been made of the concern that some individuals do not read or understand authorizations and other types of mandated forms and disclosures,[146] this concern does not obviate the ethical obligation of a researcher, regardless of whether the researcher is affiliated or independent, to request permission to use an individual's data for research and to respect the individual's decision.[147] For these reasons, this Article strongly recommends that future regulation of independent, mobile-app-based research be guided by a principle that is analogous to the HIPAA Privacy Rule's third use and disclosure requirement. That is, this Article strongly recommends that independent scientists obtain some form of prior written permission of prospective research participants to use and disclose their data for current and future research purposes.[148]

The HIPAA Privacy Rule requires authorizations for research to contain a number of core elements and required statements.[149] Most of these elements and statements are relevant to the context of independent, mobile-app-based research and should be included in authorization forms signed by prospective research participants. Specifically, this Article argues that each prospective mobile research participant should be told (1) the name or other

144 *See id.* § 164.508(a)(1).

145 *But see id.* § 164.512(i) (listing four research exceptions to the prior authorization requirement). Unless mobile-app-mediated research falls into one of these four exceptions, the third use and disclosure requirement applies, and the prior written authorization of the individuals who participate in the research is necessary.

146 *See generally* OMRI BEN-SHAHAR & CARL E. SCHNEIDER, MORE THAN YOU WANTED TO KNOW 3–54, 55–118 (2014) (arguing that mandated disclosures routinely fail to achieve their desired goals).

147 *See* Mark A. Rothstein, *Improve Privacy in Research by Eliminating Informed Consent? IOM Report Misses the Mark*, 37 J.L. MED. & ETHICS 507 (2009) (arguing that a recommendation of the Institute of Medicine that would automatically convert all patients into research subjects without their knowledge or consent denigrates respect for autonomy).

148 *But see* Cohen & Mello, *Big Data*, *supra* note 5, at E2 ("Patients could be presented with a blanket 'front door' authorization form and choose to sign or withhold permission. However, this approach may prove to be mere ethical window dressing. HIPAA appropriately calls such a process *authorization*, not *consent*, because patients are rarely given the information and opportunity to ask questions needed to give meaningful informed consent to future uses of their data. Even if those problems could be overcome, it is asking a great deal of patients to imagine and assess how their information may be used and what the risk of reidentification may be." (footnotes omitted)).

149 45 C.F.R. § 164.508(c)(1)–(2) (listing the core elements and required statements of a HIPAA-compliant authorization form).

specific identification of each mobile-app-mediated researcher who will be collecting, using, and/or disclosing the individual's data for research purposes; (2) the name or specific identification of each person who will be receiving the individual's data from the researcher, including backend data collectors, data processors, and/or other researchers; (3) a specific description of the individual's data that will be collected by the mobile app and used and/or disclosed by the researcher who identifies the information in a meaningful fashion; (4) a specific description of the current research project for which the individual's data will be collected, used, and/or disclosed; (5) if the researcher expects to use and/or disclose the individual's data for future research projects, information sufficient to put the individual on notice of that expectation; (6) a specific expiration date (e.g., December 31, 2020) or a relevant expiration event (e.g., "end of the research study") after which the individual's data will no longer be collected, used, and/or disclosed; (7) the electronic signature of the individual or the legal representative of the individual who is agreeing to the data collection, use, and/or disclosure; (8) the date that the individual or legal representative signed the authorization form; and (9) a description of the right of the individual or legal representative thereof to revoke the authorization together with the exceptions to the right to revoke, including when the individual's data has already been collected, used, and/or disclosed.[150] Conventional researchers who use mobile apps to conduct federally regulated health research have already considered how best to deliver mandated disclosures to remote research participants.[151] These online processes could be adapted by independent researchers as well.

The above discussion showed how the HIPAA Privacy Rule's use and disclosure requirements may be used as a reference point for considering options for the future regulation of independent, mobile-app-based research. Somewhat like the HIPAA Privacy Rule, which allows non-TPO and non-oral-agreement uses and disclosures to be made only with prior written authorization, the GDPR establishes consent as one among a number of alternatives that must take place before the processing of personal data is lawful.[152] According to the GDPR, consent "should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement."[153] The GDPR further clarifies that consent can include

150 *See id.*(requiring these elements and statements). *See generally* U.S. DEP'T HEALTH & HUMAN SERVS., GUIDANCE ON HIPAA AND INDIVIDUAL AUTHORIZATION OF USES AND DISCLOSURES OF PROTECTED HEALTH INFORMATION FOR RESEARCH (2018) (responding to the 21st Century Cures Act's requirement that the HHS Secretary publish guidance regarding future research authorizations).

151 *See generally* Moore et al., *supra* note 3, at figs. 2–3 (showing how Duke University uses a mobile research app to deliver mandated disclosures to remotely located research participants and to obtain their electronic signatures).

152 GDPR, *supra* note 127, art. 6.

153 *Id.* pmbl., para. 32.

the "ticking [of] a box when visiting an internet website, choosing technical settings for information society services or another statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of his or her personal data."[154] The GDPR warns, however, that "[s]ilence, pre-ticked boxes or inactivity should not therefore constitute consent."[155] With respect to the content of the consent, the GDPR would require the data subject to be aware of, at least, "the identity of the controller and the purposes of the processing for which the personal data are intended."[156] These two consent content elements mirror two of the core authorization elements required by the HIPAA Privacy Rule.[157]

The above paragraph sets forth the GDPR's requirements relating to consent when the processing involves personal data. If the data processed meets the definition of personal "data concerning health," then the data subject must give "explicit" consent unless an exception applies.[158] The GDPR defines personal data concerning health as "all data pertaining to the health status of a data subject which reveal information relating to the past, current or future physical or mental health status of the data subject."[159] According to the GDPR, this includes "any information on, for example, a disease, disability, disease risk, medical history, clinical treatment or the physiological or biomedical state of the data subject independent of its source."[160] Exceptions to explicit consent exist for processing necessary for "preventive or occupational medicine," "reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices," or "scientific or historical research purposes" to the extent such purposes are "proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject."[161]

Because Kinsey Reporter, ActiveDay, PatientsLikeMe, and MyFitnessPal collect personal data regarding physiological and/or biomedical states,[162] then the explicit-consent requirement in the GDPR would seem to apply unless a relevant exception to the explicit-consent requirement also applied. These apps could attempt to rely on the exception for scientific research purposes.[163] In this case, however, the GDPR would still require the apps to "respect the essence of the right to data protection and provide for suitable

154 *Id.*
155 *Id.*
156 *Id.* pmbl., para. 42.
157 *See* 45 C.F.R. § 164.508(c)(1)(ii), (iv) (2018).
158 GDPR, *supra* note 127, art. 9(1)–(2)(a).
159 *Id.* pmbl., para. 35.
160 *Id.*
161 *Id.* art. 9(2)(h)–(j).
162 *See* text accompanying *supra* notes 63–64, 70.
163 GDPR, *supra* note 127, art. 9(2)(j).

and specific measures to safeguard the fundamental rights and interests of the data subject"[164] and obtain general consent.

In summary, both the HIPAA Privacy Rule and the GDPR require permission (called authorization and consent, respectively) before PHI and personal data concerning health can be used, disclosed, or processed by a regulated entity. Likewise, this Article strongly recommends that independent scientists obtain the prior, explicit permission of their mobile research participants before their information is used, disclosed, or processed for research or commercial purposes. This Article recommends that the content of this permission be guided by the required content of HIPAA-compliant authorization forms.

2. Individual Rights

In addition to its use and disclosure requirements, the HIPAA Privacy Rule also contains a second set of regulations establishing certain rights for individuals who are the subject of PHI vis-à-vis their covered entities, including the rights to receive a notice of privacy practices,[165] request additional privacy protections,[166] access their PHI,[167] request amendments of incorrect or incomplete PHI,[168] and receive accountings of PHI disclosures.[169] The GDPR establishes somewhat similar rights for personal data subjects vis-à-vis their data controllers, including the rights to confirm personal data processing,[170] rectify inaccurate personal data,[171] erase personal data,[172] restrict processing,[173] and object to processing,[174] among others.

All of these rights are potentially important in the context of mobile-app-mediated health research. This Article argues that certain of these rights, including the HIPAA Privacy Rule's right to receive a notice of privacy practices and the GDPR's right to confirm personal data processing, rectify inaccurate personal data, and object to processing, are particularly important. For example, potential research participants should be informed through a notice of privacy practices regarding how their mobile apps will collect, use, and disclose their information for research; the rights that the research participants have with respect to those collection, use, and disclosure practices; and a means for research participants to complain if their rights are violated. By further example, research participants who enter incorrect research data into their mobile apps, or whose smart phones are

164 *Id.*
165 45 C.F.R. § 164.520 (2018).
166 *Id.* § 164.522.
167 *Id.* § 164.524.
168 *Id.* § 164.526.
169 *Id.* § 164.528.
170 GDPR, *supra* note 127, art. 15.
171 *Id.* art. 16.
172 *Id.* art. 17.
173 *Id.* art. 18.
174 *Id.* art. 21.

used by family members or friends when data is being collected, should have the opportunity to rectify the incorrect data entered or collected. In addition, research participants who no longer wish to participate in research should have the opportunity to object to the future collection of research data through their mobile apps.

3. Administrative Requirements

In addition to the use and disclosure requirements and the individual rights, both the HIPAA Privacy Rule and the GDPR contain a third set of requirements known as the administrative requirements. In particular, the HIPAA Privacy Rule requires covered entities to designate a privacy officer who will oversee compliance with the HIPAA Privacy Rule, train workforce members regarding how to comply with the HIPAA Privacy Rule, sanction workforce members who violate the HIPAA Privacy Rule, establish a complaint process for individuals who believe their privacy rights have been violated, and develop privacy-related policies and procedures, among other similar requirements.[175] Likewise, the GDPR requires data controllers and processors to designate a data protection officer who has expert knowledge of data protection laws and practices,[176] train staff involved in data processing,[177] allow data subjects to lodge complaints with supervisory authorities,[178] and develop policies and procedures designed to meet the principles of privacy by design and protection by default,[179] among other similar requirements.

All of these administrative requirements are important in the context of independent, mobile-app-mediated research, and this Article strongly recommends their application. A privacy official (or data protection officer) is needed to establish privacy as a key component of mobile-app-mediated research protocols and to ensure compliance with industry standards and best practices. Privacy policies and procedures should be implemented and guide the mobile collection, use, and disclosure of research data. Research participants whose data is misused should have the right to complain, and independent researchers should have the obligation to respond to and resolve those complaints.

C. Security

So far, this Article has focused on research-participant privacy and research-data confidentiality in the context of mobile-app-mediated research. Data security is also important. The HIPAA Security Rule requires covered entities and business associates to implement administrative, physical, and technical safeguards designed to protect the confidentiality, integrity, and

175 45 C.F.R. § 164.530 (2018).
176 GDPR, *supra* note 127, art. 37(1), (5).
177 *Id.* art. 39.
178 *Id.* art. 77.
179 *Id.* pmbl., para. 78.

availability of electronic, protected health information (ePHI).[180] The GDPR also requires data controllers and processors to secure networks and information with a focus on resisting "accidental events or unlawful or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted personal data."[181]

In particular, the HIPAA Security Rule's administrative requirements obligate covered entities and business associates to designate a security official responsible for the development and implementation of the covered entity's or business associate's security policies and procedures.[182] These policies and procedures shall (1) prevent, detect, contain, and correct security violations; (2) ensure that workforce members have appropriate access to ePHI; (3) prevent workforce members who should not have access to ePHI from obtaining such access; (4) create a security awareness and training program for all workforce members; and (5) address and respond to security incidents, emergencies, environmental problems, and other occurrences such as fires, vandalism, system failures, and natural disasters that affect systems containing ePHI and the security of ePHI, among other requirements.[183] Somewhat similarly, the GDPR requires data controllers and processors to (1) adopt internal policies and implement measures that meet the principles of data protection by design and data protection by default;[184] (2) evaluate the security risks inherent in the processing of personal data and implement measures to mitigate those risks;[185] (3) raise awareness regarding security issues and train staff involved in data processing operations;[186] and (4) respond to physical and technical incidents that affect the ability of data subjects to access their personal data,[187] among other requirements.

In terms of physical safeguards, the HIPAA Security Rule requires covered entities and business associates to implement policies and procedures that (1) limit physical access to electronic information systems and the facilities in which they are located; (2) address the safeguarding, functioning, and physical attributes of workstations through which ePHI is accessed; and (3) govern the receipt and removal of hardware and electronic media that contain ePHI.[188] Somewhat similarly, the GDPR requires policies and procedures designed to prevent unauthorized access to electronic communications

180 45 C.F.R. § 160.103 (2018) (defining ePHI); *id.* §§ 164.302–.310 (establishing the security obligations of covered entities and business associates). *See generally* Sharona Hoffman & Andy Podgurski, *In Sickness, Health, and Cyberspace: Protecting the Security of Electronic Private Health Information*, 48 B.C. L. REV. 331 (2007) (summarizing and critiquing the HIPAA Security Rule).

181 GDPR, *supra* note 127, pmbl., para. 49.

182 45 C.F.R. § 164.308.

183 *Id.*

184 GDPR, *supra* note 127, pmbl., para. 78.

185 *Id.* pmbl., para. 83.

186 *Id.* art. 39(1)(b).

187 *Id.* art. 32(1)(c).

188 45 C.F.R. § 164.310 (2018).

networks and damage to computer and electronic communications systems.[189]

In terms of technical safeguards, the HIPAA Security Rule requires covered entities and business associates to implement (1) technical policies and procedures for electronic information systems that maintain ePHI to allow access only to those persons or software programs that have been granted access rights; (2) hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI; (3) policies and procedures to protect ePHI from improper alteration or destruction; (4) procedures to verify that a person or entity seeking access to ePHI is the one claimed; and (5) technical security measures to guard against unauthorized access to ePHI that is being transmitted over an electronic communications network.[190] Similarly, the GDPR requires data controllers and processors to implement appropriate technical measures to protect data security including, but not limited to (1) the encryption of personal data;[191] (2) the verification of data subjects who request online access to their personal data;[192] and (3) the technical ability to restore the availability and access to personal data in the event of a physical or technical incident,[193] among other requirements.

Data security is extremely important in the context of health research, including independent, mobile-app-mediated research. A lack of security can be devastating for the privacy of research participants and the confidentiality of their sensitive research data. For example, Feinstein Institutes for Medical Research, a biomedical research institute based in Manhasset, New York, recently agreed to pay HHS $3.9 million to settle potential violations of the HIPAA Security Rule after the unsecured ePHI of approximately 13,000 research participants was stolen.[194] The stolen ePHI included research participants' names, dates of birth, addresses, social security numbers, diagnoses, laboratory results, medications, and medical information relating to their research participation.[195]

A government investigation revealed that Feinstein had security measures that were insufficient to protect the confidentiality, integrity, and availa-

189 GDPR, *supra* note 127, art. 49.

190 45 C.F.R. § 164.312.

191 GDPR, *supra* note 127, art. 32(1)(a).

192 *Id.* pmbl., para. 64.

193 *Id.* art. 32(1)(c).

194 U.S. Dep't Health & Human Servs., Resolution Agreement with Feinstein Institute for Medical Research, at (I)–(II) (2016), [hereinafter Feinstein Resolution Agreement], https://www.hhs.gov/sites/default/files/fimr-resolution-agreement-and-corrective-action-plan.pdf.

195 Press Release, U.S. Dep't Health & Human Servs., Improper Disclosure of Research Participants' Protected Health Information Results in $3.9 Million HIPAA Settlement (Mar. 17, 2016) [hereinafter Feinstein Press Release], https://wayback.archive-it.org/3926/20170127191441/https://www.hhs.gov/about/news/2016/03/17/improper-disclosure-research-participants-protected-health-information-results-in-hipaa-settlement.html.

bility of Feinstein's ePHI.[196] Illustrative examples of Feinstein's insufficient security measures included (1) a lack of policies and procedures authorizing access to ePHI by workforce members; (2) an absence of safeguards restricting access to ePHI by unauthorized users; (3) a lack of policies and procedures governing the receipt and removal of laptops containing ePHI; and (4) the failure to implement measures to encrypt ePHI or to document why encryption was unnecessary in Feinstein's research enterprise.[197] In its press release announcing the Feinstein settlement, HHS stated that "[f]or individuals to trust in the research process and for patients to trust in [research] institutions, they must have some assurance that their information is kept private and secure."[198] Because a security breach similar to the Feinstein breach could reoccur in the context of a mobile-app-mediated research project, this Article strongly recommends the application to independent, mobile-app-mediated researchers of security standards similar to those set forth in the HIPAA Security Rule and the GDPR.

D. Breach Notification

In addition to privacy and security standards, both the HIPAA Rules and the GDPR contain breach notification standards. In particular, the HIPAA Breach Notification Rule requires covered entities, following the discovery of a breach[199] of unsecured protected health information (uPHI),[200] to notify each individual whose uPHI has been, or is reasonably believed by the covered entity to have been, accessed, acquired, used, or disclosed as a result of such breach.[201] The notification, which shall be provided without undue delay and within sixty calendar days after the discovery of the breach, shall include (1) a brief description of the nature of the breach, including the date of the breach and the date of its discovery if known; (2) a description of the types of uPHI involved in the breach; (3) any steps the individual should take to protect herself from potential harm resulting from the breach; (4) a brief description of the steps taken by the covered entity to investigate the breach, to mitigate harm to individuals whose uPHI was part of the breach, and to protect against future breaches; and (5) contact information sufficient to allow individuals to ask questions or learn additional information about the breach.[202]

When a breach involves the uPHI of more than 500 residents of a state or jurisdiction, the HIPAA Breach Notification Rule also requires the covered

196 FEINSTEIN RESOLUTION AGREEMENT, *supra* note 194, at (I)(2)(ii); Feinstein Press Release, *supra* note 195.

197 FEINSTEIN RESOLUTION AGREEMENT, *supra* note 194, at (I)(2)(i)–(vi); Feinstein Press Release, *supra* note195.

198 Feinstein Press Release, *supra* note195 (quoting Office for Civil Rights Director Jocelyn Samuels).

199 45 C.F.R. § 164.402 (defining breach) (2018).

200 *Id.* (defining uPHI).

201 *Id.* § 164.404(a)(1).

202 *Id.* § 164.404(b)–(c).

entity to notify prominent media outlets serving the state or jurisdiction.[203] When a breach involves the uPHI of 500 or more individuals, regardless of their states of residency, the covered entity is also required to notify the Secretary of HHS within sixty calendar days after the discovery of the breach.[204] Finally, when the breach involves the uPHI of less than 500 individuals, the covered entity is required to notify the Secretary of HHS not later than 60 calendar days after the end of the calendar year.[205]

Somewhat similar to the HIPAA Breach Notification Rule, the GDPR requires data controllers to communicate without undue delay a personal data breach[206] to the subjects of the breach when the breach is "likely to result in a high risk to the rights and freedoms of natural persons."[207] The communication shall describe the nature of the data breach, the name and contact details of the data protection officer or other contact person from whom additional information can be gathered by the data subjects about the data breach, the likely consequences of the data breach, and the measures taken or that will be taken by the data controller to respond to the data breach.[208] In addition to notifying the data subjects, the controller shall also notify the appropriate supervisory authority[209] not later than seventy-two hours after becoming aware of the breach, unless the breach is "unlikely to result in a risk to the rights and freedoms of natural persons."[210]

Breach notification is extremely important in the context of health research, including independent, mobile-app-mediated research. When researchers fail to notify participants of a data breach, the participants may lose the opportunity to protect themselves from economic, dignitary, and psychological harms. For example, Illinois-based Presence Health Network recently paid HHS a $475,000 settlement amount following its failure to make timely breach notifications.[211] As background, HHS received a breach notification report from Presence on January 31, 2014, stating that Presence discovered on October 22, 2013, that paper-based operating-room schedules containing the PHI of 836 individuals were missing from a surgery center located in Joliet, Illinois.[212] The PHI included the individuals' names, dates of birth, medical-record numbers, dates of procedures, types of procedures,

203 *Id.* § 164.406(a).

204 *Id.* § 164.408(b).

205 *Id.* § 164.408(c).

206 GDPR, *supra* note 127, art. 4(12) (defining personal data breach as a "breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed").

207 *Id.* art. 34(1).

208 *Id.* art. 34(2).

209 *Id.* art. 51 (requiring each member state to provide for one or more independent public authorities, called supervisory authorities, to be responsible for monitoring the application of GDPR).

210 *Id.* art. 33(1).

211 *See* PRESENCE RESOLUTION AGREEMENT, *supra* note 9, at 2–3.

212 *Id.* at 1–2.

surgeon names, and types of anesthesia.[213] Although the HIPAA Breach Notification Rule requires notification to be provided without undue delay and within 60 calendar days after the discovery of the breach, Presence's breach notification process took substantially longer—approximately 101 calendar days.[214] A government investigation further revealed Presence's failure to timely notify individuals in two additional breach cases, taking approximately 104 days and 106 days from the date of discovery instead of the mandatory 60 days.[215] In its press release announcing the settlement, HHS stated that "[i]ndividuals need prompt notice of a breach of their unsecured PHI so they can take action that could help mitigate any potential harm caused by the breach."[216]

As discussed above, the HIPAA Breach Notification Rule applies to neither Kinsey Reporter, ActiveDay, PatientsLikeMe, nor MyFitnessPal.[217] The GDPR's breach communication rule does apply to PatientsLikeMe and MyFitnessPal but would not apply to non-EU-established researchers whose mobile apps only monitor the behavior of data subjects outside the European Union. This Article strongly recommends that all mobile-app-based researchers be required to timely notify their research participants of data breaches to help protect against economic, dignitary, and psychological harms.

III. State Survey Results

As discussed in Part II, the HIPAA Rules will not apply to many independent scientists who conduct or participate in mobile-app-mediated health research. Although the GDPR may apply to some apps that monitor behavior that takes place in the European Union, some apps developed in the United States that monitor behavior are used only by individuals located in the United States. Neither the HIPAA Rules nor the GDPR, therefore, can be relied on to establish standards applicable to all health data gathered by mobile research apps. In addition, the HIPAA Rules are outdated in terms of their concentrated focus on the treatment, payment, healthcare operations, and other activities of traditional health industry participants.

This Part III responds to this limitation by assessing nonsectoral state statutes that are potentially applicable to mobile-app-mediated research conducted by independent scientists. If applicable federal standards do not exist or are outdated, and if the federal government fails to enact or enforce new standards, perhaps state law can fill the gap in the meantime. The state stat-

213 Press Release, U.S. Dep't Health & Human Servs., First HIPAA Enforcement Action for Lack of Timely Breach Notification Settles for $475,000 (Jan. 9, 2017) [hereinafter Presence Press Release], http://wayback.archive-it.org/3926/20170127111957/https://www.hhs.gov/about/news/2017/01/09/first-hipaa-enforcement-action-lack-timely-breach-notification-settles-475000.html.

214 Presence Resolution Agreement, *supra* note 9, at 2.

215 *Id.* at 2.

216 Presence Press Release, *supra* note 213.

217 *See supra* Section II.A.

utes identified below are "potentially applicable" because they are not limited in application to certain professionals, such as physicians or bankers; certain institutions, such as hospitals, financial institutions, or government agencies; certain sources of funding, such as federal funding; or certain industries, such as the financial or health industries. By definition, the independent scientists who are the focus of this Article are not licensed healthcare professionals or bankers. They are not employed by hospitals, government agencies, or other institutions. They do not receive federal funding, and they are not tied to a particular business sector.

Because all fifty states and the District of Columbia ("states" or "state") have potentially applicable breach notification statutes[218] but fewer states have potentially applicable data security[219] and data privacy[220] statutes, breach notification statutes will be discussed first.

---

218 *See* ALA. CODE § 8-38-1 to -12 (2019); ALASKA STAT. ANN. § 45.48.010–.090 (West 2019); ARIZ. REV. STAT. ANN. §§ 18-551 to -552, 44-7601 (2019); ARK. CODE ANN. § 4-110-101 to -108 (West 2019); CAL. CIV. CODE §§ 1798.1–.78 (West 2019); COLO. REV. STAT. ANN. §§ 6-1-713 to -716 (West 2019); CONN. GEN. STAT. ANN. §§ 36a-701a to -701b, 42-471 (West 2019); DEL. CODE ANN. tit. 6, §§ 12B-100 to -104, 5001C (West 2019); D.C. CODE ANN. §§ 28-3851 to -3853 (West 2019); FLA. STAT. ANN. § 501.171 (West 2019); GA. CODE ANN. §§ 10-1-910 to -912, -15-2 (West 2019); HAW. REV. STAT. ANN. §§ 487N-1 to -3, 487R-2 (West 2019); IDAHO CODE ANN. §§ 28-51-104 to -107 (West 2019); 815 ILL. COMP. STAT. ANN. 530/1–50 (West 2019); IND. CODE § 24-4.9-1-1 to .9-5-1 (West 2019); IOWA CODE ANN. §§ 715C.1–.2 (West 2019); KAN. STAT. ANN. §§ 50-6,139b, -7a01–04 (West 2019); KY. REV. STAT. ANN. §§ 365.720–.734 (West 2019); LA. STAT. ANN. §§ 51:3071 to :3074 (2019); ME. REV. STAT. ANN. tit. 10, §§ 1346–1350-B (West 2019); MD. CODE ANN., COM. LAW §§ 14-3501 to -3508 (West 2019); MASS. GEN. LAWS ANN. ch. 93H, §§ 1–6 (West 2019); MICH. COMP. LAWS ANN. §§ 445.63–.79d (West 2019); MINN. STAT. ANN. § 325E.61 (West 2019); MISS. CODE ANN. § 75-24-29 (West 2019); MO. ANN. STAT. § 407.1500 (West 2019); MONT. CODE ANN. §§ 30-14-1701 to -1736 (West 2019); NEB. REV. STAT. ANN. §§ 87-801 to -808 (West 2019); NEV. REV. STAT. ANN. §§ 603A.010–.290 (West 2019); N.H. REV. STAT. ANN. §§ 359-C:19–21 (2019); N.J. STAT. ANN. §§ 56:8-161 to -163 (West 2019); N.M. STAT. ANN. §§ 57-12c-1 to -12 (West 2019); N.Y. GEN. BUS. LAW §§ 899-aa, -bb (McKinney 2019); N.C. GEN. STAT. ANN. §§ 75-60 to -66 (West 2019); N.D. CENT. CODE ANN §§ 51-30-01 to -07 (West 2019); OHIO REV. CODE ANN. §§ 1349.19, .191–.192, 1354.01 (West 2019); OKLA. STAT. ANN. tit. 24, §§ 161–166 (West 2019); OR. REV. STAT. ANN. §§ 646A.600–.628 (West 2019), *amended by* Act of May 24, 2019, 2019 Or. Laws ch. 180, S.B. 684; 73 PA. STAT. AND CONS. STAT. §§ 2301–2309 (West 2019); 11 R.I. GEN. LAWS ANN §§ 6-52-2, 11-49.3-1 to -6 (West 2019); S.C. CODE ANN. § 39-1-90 (2019); S.D. CODIFIED LAWS §§ 22-40-19 to -26 (2019); TENN. CODE ANN. §§ 39-14-150(g), 47-18-2101 to -2111 (West 2019); TEX. BUS. & COM. CODE ANN. §§ 521.002, .053 (West 2019); UTAH CODE ANN. § 13-44-101 to -301 (West 2019); VT. STAT. ANN. tit. 9 §§ 2430–2445 (West 2019); VA. CODE ANN. § 18.2-186.6 (West 2019); WASH. REV. CODE §§ 19.215.020, .255.010 (2019), *amended by* Act of May 7, 2019, 2019 Wash. Legis. Serv. ch. 241, S.H.B. 1071 (West) (to be codified in scattered sections of WASH. REV. CODE) (effective Mar. 1, 2020); W. VA. CODE ANN §§ 46A-2A-101 to -105 (West 2019); WIS. STAT. ANN. §§ 134.97–.98 (West 2019); WYO. STAT. ANN. §§ 40-12-501 to -509 (West 2019); California Consumer Privacy Act of 2018, 2018 Cal. Legis. Serv. ch. 55, A.B. 375 (West) (to be codified at CAL. CIV. CODE §§ 1798.100–.198) (effective Jan. 1, 2020)), *amended by* 2018 Cal. Legis. Serv. ch. 735, S.B. 1121 (West); 201 MASS. CODE REGS. 17.01–.05 (2019).

219 *See infra* note 257 (listing the states that have nonsectoral data security statutes).

A. State Breach Notification Laws

This Article finds that fifty-one (100%) of fifty-one states have enacted data breach notification statutes that are potentially applicable to independent scientists who conduct mobile-app-mediated health research.[221] At the outset, this Article notes that the fifty-one statutes originally had a wide variety of names, suggesting different purposes and scopes. For example, thirteen (25.5%) of the fifty-one laws contain the phrase "identity theft" or "identity crimes" in their formal or popular names, suggesting that protection against identity theft and associated economic harm is the primary, or an important, purpose of the legislation.[222] Twenty-three (45.1%) of the fifty-one laws contain the phrase "breach," "data breach," "security breach," "breach of security," "notice of breach," "breach notice," "notice of risk," or "notice of unauthorized acquisition" in their formal or popular names, suggesting that notifying individuals that their data has been accessed without authorization is the primary or an important purpose of the legislation.[223] Thirteen (25.5%) of the fifty-one laws contain the phrase "personal data," "personal information," "financial information," "information protection," "information practices," "consumer data privacy," or "consumer records" in their formal or popular names, suggesting that the protection of information more generally is an important purpose of the legislation.[224]

Regarding content, all fifty-one (100%) of the breach notification statutes contain individual breach notification provisions; that is, provisions requiring notification of state residents, consumers, or other individuals whose data was the subject of a security breach, depending on the circum-

220 *See* CAL. BUS. & PROF. CODE §§ 22575–22579 (West 2019); CAL. CIV. CODE §§ 1798.83–.84 (West 2019); CAL. HEALTH & SAFETY CODE §§ 24170–24178 (West 2019); DEL. CODE ANN. tit. 6 §§ 1201c–1206c (West 2019); FLA. STAT. ANN. § 381.026(4)(e) (West 2019); 410 ILL. COMP. STAT. ANN. 50/3.1(a) (West 2019); MD. CODE ANN., HEALTH–GEN. § 13-2002 (West 2019); NEB. REV. STAT. ANN. § 87-302(15) (West 2019); NEV. REV. STAT. ANN. §§ 603A.300–.360 (West 2019); N.J. STAT. ANN. § 26:14-4 (West 2019); N.Y. PUB. HEALTH LAW §§ 2440–2446 (McKinney 2019); OR. REV. STAT. § 646.607(12) (West. 2019); 18 PA. STAT AND CONS. STAT. ANN. § 4107(a)(10) (West 2019); TEX. HEALTH & SAFETY CODE ANN. §§ 181.001–.207 (West 2019); UTAH CODE ANN. §§ 13-37-101 to -102 (West 2019); VA. CODE ANN. §§ 32.1-162.16–.20 (West 2019); California Consumer Privacy Act of 2018, 2018 Cal. Legis. Serv. ch. 55, A.B. 375 (West) (to be codified at CAL. CIV. CODE §§ 1798.100–.198) (effective Jan. 1, 2020), *amended by* 2018 Cal. Legis. Serv. ch. 735, S.B. 1121 (West).

221 *See* sources cited *supra* note 218.

222 The states with such laws are Connecticut, Georgia, Idaho, Iowa, Louisiana, Michigan, Montana, North Carolina, Oregon, Rhode Island, South Carolina, Tennessee, and Texas. *See* sources cited *supra* note 218.

223 The states with such laws are Alabama, Arizona, Delaware, District of Columbia, Hawaii, Indiana, Louisiana, Massachusetts, Minnesota, Mississippi, Missouri, Nebraska, New Mexico, New York, North Dakota, Ohio, Oklahoma, Pennsylvania, South Dakota, Virginia, West Virginia, Wisconsin, and Wyoming. *See* sources cited *supra* note 218.

224 The states with such laws are Alaska, Arkansas, Colorado, Florida, Georgia, Illinois, Idaho, Kentucky, Maryland, Nevada, Utah, Vermont, and Washington. *See* sources cited *supra* note 218.

stances of the breach.[225] Approximately two-thirds of the state laws require notification of consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, depending on the circumstances of the breach.[226] Approximately three-fifths of the state laws also require notification of the states' attorneys general, departments of legal affairs, offices of consumer protection, and/or police, depending on the circumstances of the breach.[227] More than ninety percent of state laws require a third-party agent, data storage company, data processor, data nonowner, or data nonlicensee to notify the appropriate regulated entity, data controller, data owner, or data licensee of the breach, depending on the circumstances of the breach.[228]

These breach notification provisions are very similar in purpose and effect to those set forth in the HIPAA Breach Notification Rule and the GDPR, as discussed in Section II.D.[229] That is, these state provisions are designed to alert both the individual who is the subject of the data as well as an appropriate governmental agency of a data breach, thus enabling the individual to take self-protection measures while also providing at least one government agency the opportunity to respond and/or monitor compliance.

Moving from content to application, these laws tend to have broad, but not unlimited, application. For example, Alabama's Data Breach Notification Act of 2018 applies to individuals and institutions that fall within the Act's definition of a "covered entity."[230] The Alabama law defines a covered entity as a "person, sole proprietorship, partnership, government entity, corporation, nonprofit, trust, estate, cooperative association, or other business entity that acquires or uses sensitive personally identifying information."[231] The Alabama law defines "sensitive personally identifying information" as an Alabama resident's first name or first initial and last name together with other sensitive information including, but not limited to, medical history, mental condition, physical condition, medical treatment, or diagnosis.[232]

225 *See* sources cited *supra* note 218.

226 The states requiring notice to consumer reporting agencies are Alabama, Alaska, Arizona, Colorado, District of Columbia, Florida, Georgia, Hawaii, Indiana, Kansas, Kentucky, Maine, Maryland, Massachusetts, Michigan, Minnesota, Missouri, Montana, Nevada, New Hampshire, New Mexico, New York, North Carolina, Ohio, Oregon, Pennsylvania, Rhode Island, South Carolina, South Dakota, Tennessee, Texas, Vermont, Virginia, West Virginia. *See* sources cited *supra* note 218.

227 The states requiring notice to a state agency are Alabama, Alaska, Arizona, California, Colorado, Connecticut, Delaware, Florida, Hawaii, Idaho, Illinois, Indiana, Iowa, Maine, Maryland, Massachusetts, Missouri, Montana, Nebraska, New Hampshire, New Mexico, New York, North Carolina, North Dakota, Oregon, Rhode Island, South Carolina, South Dakota, Texas, Vermont, Virginia, and Washington. *See* sources cited *supra* note 218.

228 All states except Alaska, Connecticut, Indiana, Rhode Island, South Dakota, Texas, and Utah require some third-party involvement. *See* sources cited *supra* note 218.

229 *See supra* Section II.D (discussing the HIPAA Breach Notification Rule and the GDPR's breach notification provisions).

230 *See* ALA. CODE § 8-38-2 (2019).

231 *Id.*

232 *Id.*

An independent scientist is certainly a person and could also be a sole proprietor, thus meeting the first part of the Alabama law's definition of covered entity. Depending on the mobile-app-mediated research project, however, the independent scientist may or may not be acquiring or using sensitive personally identifying information as necessary for regulation to occur. In the hypothetical that opened this Article, recall the independent scientist who developed a disease-progression mobile research app that collected each research participant's full name, date of birth, diagnosis, and medications, among other data elements.[233] If any of the disease-progression research participants who used the independent scientist's app were Alabama residents, the independent scientist would be acquiring and using sensitive personally identifying information for purposes of the Alabama law.

Compare, however, Kinsey Reporter, which collects neither the name (nor any type of user identity) nor precise geolocation of its citizen sex scientists, but does collect data regarding the city, state, and country (e.g., "Seminole, Florida, US") where the reported sexual health issue or intimate behavior occurred, as well as the age, gender, and IP address of the reporting citizen sex scientist.[234] Because the Alabama law only protects information that is tied to the first name or first initial and last name of a data subject, the Alabama law would not apply to Kinsey Reporter. This is true even if a potentially reidentifiable resident of a very small Alabama town shared the resident's sexual health data with Kinsey Reporter and the security of that sexual health data was subsequently breached.

As of this writing, more than two-thirds of other states' breach notification laws share this limitation. That is, more than two-thirds of other states only protect data that is tied to the first name or first initial and last name of a data subject although other information, such as an individual's mailing address, geolocation, email address, telephone number, or photograph, could be used to identify the data subject.[235] These breach notification laws fail to recognize that "[t]he aggregation and correlation of data from various sources make it increasingly possible to link supposedly anonymous information to specific individuals and to infer characteristics and information about them."[236] Stated another way, these breach notification laws have not kept

233 *See* text accompanying *supra* note 3.

234 *See supra* notes 40–41 and accompanying text.

235 Those states are Alaska, Arkansas, Colorado, Connecticut, Delaware, District of Columbia, Hawaii, Idaho, Indiana (which also allows social security number to suffice), Iowa, Kansas, Kentucky, Louisiana, Massachusetts, Michigan, Minnesota, Mississippi, Missouri, Nevada, New Hampshire, New Jersey, New Mexico, North Carolina, North Dakota, Ohio, Oklahoma, Oregon, Pennsylvania, Rhode Island, South Carolina, Tennessee, Utah, Virginia, Washington, West Virginia, and Wyoming. *See* sources cited *supra* note 218.

236 *See, e.g.*, Cameron F. Kerry, *Why Protecting Privacy Is a Losing Game Today—and How to Change the Game*, BROOKINGS INSTITUTION (July 12, 2018), https://www.brookings.edu/research/why-protecting-privacy-is-a-losing-game-today-and-how-to-change-the-game/ ("To most people, 'personal information' means information like social security numbers, account numbers, and other information that is unique to them. U.S. privacy laws reflect this conception by aiming at 'personally identifiable information,' but data scientists have

up with big data's ability to reidentify individuals with nonobvious identifiers.[237]

Other states, however, have crafted slightly broader definitions of protected data. Montana, for example, defines personal information as "an individual's name, signature, address, or telephone number, in combination with" other information,[238] thus recognizing that an individual's signature, address, or telephone number could also be used to identify an individual. In counties with publicly accessible property records, for example, an individual's address can quickly reveal the first and last name of the data subject if the subject is the only person who owns and lives at the property.

Texas's law, by further example, allows "an individual's first name or first initial and last name in combination with" certain other data to constitute "[s]ensitive personal information."[239] Texas's law also protects, however, any other "information that identifies an individual and relates . . . to the physical or mental health or condition of the individual."[240] Texas's law is similar to the HIPAA Rules,[241] which recognize that first name or first initial and last name are not the only ways individuals can be recognized. This Article recommends that the law of Alabama (and the laws of the other states that are similar to Alabama) be amended to include a laundry list of identifiers, similar to that set forth in the HIPAA Privacy Rule,[242] but expanded given advances in big data, so that all health data subjects, even those who do not provide their first names or first initials and last names, are protected.

Other minor limitations in state laws prevent their application to all independent scientists who conduct mobile-app-mediated health research. Kansas's data breach provisions, for example, only apply when the data breach involves data that is linked to an unencrypted and unredacted social

---

repeatedly demonstrated that this focus can be too narrow. The aggregation and correlation of data from various sources make it increasingly possible to link supposedly anonymous information to specific individuals and to infer characteristics and information about them. The result is that today, a widening range of data has the potential to be personal information, i.e. to identify us uniquely. Few laws or regulations address this new reality.").

237 *Id.*; *see also* Cohen & Mello, *Big Data*, *supra* note 5 ("When HIPAA was adopted in 1996, . . . Google did not exist, the global internet had about 100,000 websites, and geolocation tracking was available only for the military. . . . Personal data were presumed nonidentifiable if stripped of 18 identifiers, most of which were direct identifiers . . . . The substantial increase in available personal information and advances in computing mean that individuals can often be identified in deidentified data by triangulating data sources.").

238 MONT. CODE ANN. § 30-14-1702 (West 2019).

239 TEX. BUS. & COM. CODE ANN. § 521.002(a)(2)(B)(i) (West 2019).

240 *Id.*

241 *See* 45 C.F.R. § 160.103 (2018) (defining protected health information (PHI) based on individually identifiable health information (IIHI), and defining IIHI to include information relating to the "past, present, or future physical or mental health or condition of an individual").

242 *See id.* § 164.514(b)(2)(i)(A)–(R) (listing eighteen identifiers that must be removed from health information in order for the information to be considered deidentified under the HIPAA Privacy Rule).

security number, driver's license number, state identification card number, financial account number, or credit or debit card number.[243] Kansas was probably focused on the economic harms associated with identity theft when it drafted its legislation. Kansas's legislation fails to recognize, however, the dignitary and psychological harms associated with the unwanted disclosure of sensitive and stigmatizing health information.

Alabama's law picks up where Kansas's law left off by including within its definition of "sensitive personally identifying information" data linked to medical history, physical condition, mental condition, medical treatment, or diagnosis.[244] Alabama's inclusion of "physical condition" and "diagnosis" would pull in, for example, the sexual health data collected by Kinsey Reporter, the fall and first-responder data collected by ActiveDay and Fall-Safety Pro, the terminal and other serious diagnoses of the PatientsLikeMe registrants, and the weight, exercise, and nutrition data collected by MyFitnessPal. Because some data—including data collected outside the context of mobile research apps—does not relate to health but, instead, relates to products or services purchased, consumer tendencies, electronic network activity information, internet browsing activity, and other nonpublic consumer preferences, characteristics, psychological trends, preferences, predispositions, behaviors, attitudes, intelligence, abilities, and aptitudes, states should consider protecting these data elements as well.

Still other minor limitations in state laws become apparent when applied to independent scientists who conduct mobile-app-mediated research. Georgia's law, for example, applies to "data collector[s]" and "information broker[s]."[245] "Data collector[s]," under Georgia law, are state and local agencies. "Information broker[s]" are "person[s] . . . who, for monetary fees or dues, engage[ ] in . . . collecting, assembling, evaluating, . . . [or] transferring . . . information concerning individuals."[246] By definition, an independent scientist does not work for a state or local agency. In addition, many independent scientists do not collect fees or dues from their research participants in exchange for engaging in research using the participants' data. Neither Kinsey Reporter, ActiveDay, PatientsLikeMe, nor MyFitnessPal charges fees or dues for research participants, although some of the apps' privacy policies state that they may sell collected data to third parties for research purposes.[247] To remove questions regarding applicability, the Georgia law could be amended to apply to all natural or legal persons who collect, assemble, evaluate, or transfer personal information regardless of when or whether any remuneration is involved.

---

243 KAN. STAT. ANN. § 50-7a01(g) (West 2019).

244 ALA. CODE § 8-38-2(6)(a)(4) (2019).

245 GA. CODE ANN. § 10-1-912 (West 2019).

246 *Id.* § 10-1-911(2)–(3).

247 *See, e.g.*, *Terms and Conditions of Use*, PATIENTSLIKEME, https://www.patientslikeme.com/about/user_agreement (last visited Sept. 9, 2019); *Under Armour Privacy Policy*, *supra* note 69.

Still other state laws require a person or entity to be "doing business" or "conducting business" in the state before regulation occurs. New Hampshire's law, for example, applies to "any person doing business in [New Hampshire]."[248] Arizona's law similarly requires a person to be "conduct[ing] business" in Arizona for the regulation to apply.[249] Some states loosely define "doing business" or "conducting business" to include owning or using personal information of a state resident even if the person or entity doing the owning or using does not have a physical presence in the state. Indiana's law, for example, defines "[d]oing business in Indiana" as "owning or using the personal information of an Indiana resident for commercial purposes."[250] Recall that Kinsey Reporter is based in Indiana, ActiveDay in Washington, PatientsLikeMe in Massachusetts, and MyFitnessPal in Maryland.[251] The companies that created these apps may not have employees or physical presences in all states; however, they are capable of collecting data from residents of all states through their mobile apps.

Unlike Indiana, however, some states regulate persons or entities "doing business" or "conducting business" in that state, but they fail to clarify whether the collection and use of data regarding a state resident (without more) meets that standard.[252] As a result, a broad definition of "doing business"—similar to that set forth in the Indiana law—is desirable when viewed from the perspective of a participant in mobile-app-mediated research conducted by a researcher located outside the state in which the participant resides. For example, North Carolina has crafted language that regulates traditional, brick-and-mortar businesses in North Carolina, as well as mobile-app-mediated researchers. In particular, North Carolina regulates "[a]ny business that conducts business in North Carolina," as well as "any business that maintains or otherwise possesses personal information of a resident of North Carolina."[253] The second clause in the prior sentence would cover independent scientists located outside North Carolina whose mobile apps collect data from North Carolina residents.

More broadly, some states' breach notification laws apply to government agencies, large corporations, or other specific institutions, but not necessarily to natural persons. Illinois's law, for example, applies to a "data collector," defined to include "government agencies, public and private universities, privately and publicly held corporations, financial institutions, retail operators,

248 N.H. REV. STAT. ANN. § 359-C:20(I) (2019).

249 ARIZ. REV. STAT. ANN. § 18-552(A) (2019).

250 IND. CODE ANN. § 24-4.9-2-4 (West 2019).

251 *See supra* Sections I.A–D.

252 *See* 73 PA. STAT. AND CONS. STAT. ANN. § 2302 (West 2019) (applying Pennsylvania's breach notification law to an entity, defined as an individual or a business "doing business" in the Commonwealth of Pennsylvania, but not clarifying whether collecting data from a Pennsylvania resident without more is "doing business"); *see also* N.H. REV. STAT. ANN. § 359-C:20 (2019) (applying New Hampshire's breach notification law to "any person doing business in [New Hampshire]," but not clarifying whether collecting data from a New Hampshire resident without more is "doing business").

253 N.C. GEN. STAT. ANN. § 75-64 (West 2019).

and any other [business] entity that, for any purpose, handles, collects, disseminates, or otherwise deals with nonpublic personal information."[254] Other state laws, however, specifically apply to natural persons.[255] Given that many independent scientists are natural persons without governmental, corporate, or institutional status or affiliation, this Article strongly recommends that states include natural persons in their list of regulated entities.

Finally, most of the breach notification laws appear not to have contemplated the collection of data by mobile apps. However, at least one state did. Illinois's Personal Information Protection Act defines protected "[m]edical information" to include information regarding an individual's physical or mental health condition, including "information provided to a . . . mobile application."[256]

B. State Security Laws

Moving from breach notification laws to security laws, more than two-thirds of states have at least one potentially applicable data security statute.[257] These security provisions were typically either part of the same acts that established the states' breach notification provisions or codified near the states' breach notification provisions. In some cases, the persons and entities that are regulated by the security provisions are the same as those regulated by the breach notification provisions.[258] In other cases, the persons and entities regulated by the security provisions are different than those regulated by the breach notification provisions.[259] In either case, this Article's prior recommendations regarding the persons and entities regulated by breach notification provisions also apply to the persons and entities regulated by security provisions. For example, a security provision that only applies to a government agency or a large corporation should be amended so that it also applies to a natural person. By further example, a security provision that only applies to a person or entity doing business in the state should be amended

254 815 ILL. COMP. STAT. ANN. 530/5, 530/10 (West 2019).

255 *See, e.g.*, IND. CODE ANN. § 24-4.9-2-9 (West 2019) (defining person as an individual as well as a corporation).

256 815 ILL. COMP. STAT. ANN. 530/5 (West 2019) (defining "[p]ersonal information," which internally references the definition of "[m]edical information").

257 Those states are Alabama, Alaska, Arizona, Arkansas, California, Colorado, Connecticut, Delaware, Florida, Georgia, Hawaii, Illinois, Indiana, Kansas, Kentucky, Louisiana, Maine, Maryland, Massachusetts, Michigan, Montana, Nebraska, Nevada, New Jersey, New Mexico, New York, North Carolina, Ohio, Oregon, Rhode Island, South Carolina, Tennessee, Texas, Utah, Vermont, Washington, and Wisconsin. *See* sources cited *supra* note 218.

258 *See, e.g.*, ARK. CODE ANN. §§ 4-110-104 to -105 (West 2019) (setting forth a modest security law that applies to persons and businesses, which are also regulated by Arkansas's breach notification law).

259 *See, e.g.*, ALASKA STAT. ANN. §§ 45.48.010, .090, .500 (West 2019) (setting forth a security law that applies to businesses and government agencies but not persons with more than ten employees, even though persons with more than ten employees are governed by Alaska's breach notification law).

to clarify that owning or using personal data of a state resident constitutes doing business in the state.

What is notable about some of the security statutes is how modest they are when compared to the HIPAA Security Rule and the GDPR. For example, Alaska's security provision requires businesses and governmental agencies to "take all reasonable measures necessary to protect against unauthorized access to or use of records" when "disposing of records that contain personal information."[260] The law also states that reasonable measures include

> (1) implementing and monitoring compliance with policies and procedures that require the burning, pulverizing, or shredding of paper documents containing personal information so that the personal information cannot practicably be read or reconstructed;
>
> (2) implementing and monitoring compliance with policies and procedures that require the destruction or erasure of electronic media and other nonpaper media containing personal information so that the personal information cannot practicably be read or reconstructed;
>
> (3) after due diligence, entering into a written contract with a third party engaged in the business of record destruction to dispose of [such] records . . . ."[261]

Far from a comprehensive security law, Alaska's law may be properly classified as a "secure-disposal" or "secure-destruction" law. The law does not mandate any administrative, technical, or physical safeguards outside the context of the disposal or destruction of personal information. The law does not address, for example, the need for security policies and procedures addressing nondisposed data; the designation of a data security officer to oversee implementation of and compliance with such policies and procedures with respect to nondisposed data; encryption; access controls; or identifying and responding to suspected or known security incidents involving nondisposed data.

In contrast, one state (Oregon) not only requires the development, implementation, and maintenance of reasonable security safeguards, but also specifies exactly how that requirement can be satisfied, including by specifying particular administrative, technical, and physical safeguards that must be adopted.[262] A second state (Massachusetts) has delegated to a state agency the duty to promulgate comprehensive security standards, a task the agency

260 *Id.* § 45.48.500.

261 *Id.* § 45.48.510. More than two dozen additional state statutes contain similar secure-disposal or secure-destruction standards, including Arizona, Arkansas, Connecticut, Delaware, Florida, Georgia, Hawaii, Illinois, Indiana, Kansas, Kentucky, Louisiana, Maryland, Michigan, Montana, Nebraska, Nevada, New Jersey, New Mexico, New York, North Carolina, Oregon, Rhode Island, South Carolina, Tennessee, Texas, Utah, Vermont, Washington, and Wisconsin. *See* sources cited *supra* note 218.

262 *See* OR. REV. STAT. ANN. § 646A.622 (West 2019).

completed with gusto by its stated deadline.[263] A third state (Ohio) has a cybersecurity act that went into effect on November 2, 2018.[264] The Ohio legislation creates an affirmative defense for any covered entity that creates, maintains, and complies with a written cybersecurity program that includes comprehensive physical, technical, and administrative safeguards, which are set forth in the legislation, thus encouraging covered entities to implement comprehensive data security programs.[265] This Article recommends that states with modest secure-disposal statutes and states without data security statutes consider the data security approaches of Oregon, Massachusetts, and Ohio.

C. State Privacy Laws

Moving from state security statutes to state privacy statutes, less than one-third of states have at least one data privacy statute that is potentially applicable to independent scientists who conduct mobile-app-mediated research.[266] Three of these state laws may be properly classified as "online privacy policy laws." The California Online Privacy Protection Act (CalOPPA) is an illustrative example. CalOPPA requires an operator of a commercial website or online service that collects personally identifiable information about residents of California who visit the operator's website or use the operator's online service to conspicuously post a privacy policy on the website or make it available through the online service.[267] Among other requirements, the privacy policy must (1) identify the categories of personally identifiable information collected by the operator and the categories of third-party persons or entities with whom the operator may share that personally identifiable information; (2) describe any processes available for consumers to review and request changes to collected personally identifiable information; and (3) disclose whether other parties may collect personally identifiable information about a consumer's online activities over time and across different websites when a consumer uses the operator's website or service.[268] CalOPPA broadly defines personally identifiable information as "individually identifiable information about an individual consumer collected online by the operator,"

263 *See* MASS. GEN. LAWS ANN. ch. 93H, § 2 (West 2019); 201 MASS. CODE REGS. 17.01–.05 (2019).

264 *See* OHIO REV. CODE ANN. §§ 1354.01–.02 (West 2019).

265 *Id.*

266 California has four statutes, and each of the following have one: Delaware, Florida, Illinois, Maryland, Nebraska, Nevada, New Jersey, New York, Oregon, Pennsylvania, Texas, Utah, and Virginia. *See* sources cited *supra* note 220. Other states have data privacy statutes; however, they are not potentially applicable to independent researchers who conduct mobile-app-mediated health research. *See, e.g.*, Act of June 6, 2019, 2019 Me. Legis. Serv. ch. 216, S.P. 275(West) (to be codified at ME. REV. STAT. ANN. tit. 35-a, § 9301) (regulating only persons who provide broadband internet access services); VT. STAT. ANN. tit. 9, §§ 2446–2447 (West 2019) (regulating only data brokers, not first-line data collectors).

267 CAL. BUS. & PROF. CODE §§ 22575–22579 (West 2019).

268 *Id.* § 22575.

including first and last name, home or other physical address, e-mail address, telephone number, social security number, or any other identifier that permits the physical or online contacting of a specific individual.[269] Delaware and Nevada have similar online privacy policy laws. Delaware's online privacy policy law is forward thinking in that it specifically mentions its application to mobile apps.[270] Nevada's law is more limited in that it does not apply if the website or online service has fewer than 20,000 unique visitors per year.[271] Mobile research apps that serve fewer than 20,000 research participants can avoid online privacy policy regulation in states like Nevada.

Three additional state privacy laws may be properly classified as "privacy policy false statement laws." These laws, enacted in Nebraska, Oregon, and Pennsylvania, are embedded within state deceptive trade practices acts.[272] These laws classify as a deceptive or otherwise unlawful trade practice the making of a false or misleading statement regarding the use of personal information submitted by consumers in a privacy policy, including an online privacy policy.[273]

One state, Utah, has a law that requires certain persons to provide certain consumers with a notice of intent to sell their nonpublic personal information before selling their nonpublic personal information.[274] Because PatientsLikeMe and other mobile health and research apps state that they sell nonpublic health or research participant data, this law has important, potential application. However, Utah's law is limited in that it only regulates those persons that maintain an office in the state.[275] Unless a mobile-app-mediated researcher happens to have an office in Utah, the law would not apply. This Article recommends that the Utah law be amended to apply whenever a data subject is located in the state, not when the data collector offices in the state.

Five of the potentially applicable data privacy statutes[276] may be classified as "human research laws." These laws give research participants certain rights, including the right to receive information regarding studies in which they are considering enrolling, as well as the right to consent—or refuse to

269 *Id.* § 22577.

270 DEL. CODE ANN. tit. 6, §§ 1201c–1206c (West 2019); *see also* 2019 NEV. REV. STAT. ANN., §§ 603a.300–.360 (West 2019).

271 NEV. REV. STAT. ANN. § 603A.340(3)(c) (West 2019).

272 *See* NEB. REV. STAT. ANN. § 87-302(15) (West 2019); OR. REV. STAT. ANN. § 646.607(12) (West. 2019); 18 PA. STAT. AND CONS. STAT. ANN. § 4107(a)(10) (West 2019).

273 *See* NEB. REV. STAT. ANN. § 87-302(15) (West 2019); OR. REV. STAT. ANN. § 646.607(12) (West. 2019); 18 PA. STAT. AND CONS. STAT. ANN. § 4107(a)(10) (West 2019).

274 UTAH CODE ANN. §§ 13-37-101 to -203 (West 2019); *see also* CAL. CIV. CODE §§ 1798.83–.84 (West 2019) (California's "Shine the Light" law, which contains provisions somewhat similar to the Utah law).

275 UTAH CODE ANN. § 13-37-102 (West 2019).

276 Other states have research laws that are limited in application to certain classes of researchers (e.g., physician researchers) or research conducted in certain contexts (e.g., hospital-based research). *See, e.g.*, 410 ILL. COMP. STAT. ANN. 50/3.1(a) (West 2019) (applying to only physician researchers and hospital-based research).

consent—to research participation, including the use and disclosure of their data for research purposes. In particular, Maryland's research law prohibits a person from "conduct[ing] research using a human subject unless the person conducts the research in accordance with the [Federal Common Rule]."[277] (The Common Rule requires an institutional review board to ensure that researchers adequately protect research-participant privacy and research-data confidentiality.)[278] New Jersey's research law sets forth detailed requirements relating to the consent form and the consent-to-research process.[279] Virginia's research law requires researchers not subject to the Federal Common Rule (which some mobile-app-mediated researchers are not) to obtain the "legally effective informed consent" of a human research subject[280] prior to the use or disclosure of their data for research purposes. None of these statutes waives its disclosure or consent requirements in the context of online or mobile-app-mediated research.

The remaining two human research laws may not apply to all mobile-app-mediated research projects, although they are useful for policymakers to consider for drafting purposes. New York's law, which requires review and approval of research protocols by a human research review committee, as well as informed consent by research participants, only applies to research involving physical or physiological intervention on a human subject. The law specifically excludes from regulation research on withdrawn or removed fluids and tissues, as well as epidemiological research.[281] California has a similar medical experimentation law that sets forth a number of requirements, including the provision to research participants of a lengthy bill of rights and the obtaining of informed consent from research participants.[282] However, the California law only applies to "medical experiments," narrowly defined to include the "severance or penetration or damaging of tissues of a human subject," as well as the use of certain drugs, devices, and substances.[283] Some mobile-app-mediated research projects will not be regulated by the New York or California laws due to the research participants' lack of physical or physiological involvement. Note, however, that the PatientsLikeMe study did involve the participants' ingestion of a drug (lithium).

The online privacy policy laws, privacy policy false statement laws, "notice of intent to sell nonpublic personal information laws," and human research laws discussed above do not establish comprehensive privacy protections for mobile research participants. For example, they do not establish detailed data use and disclosure requirements, nor do they provide research participants with a wide range of legal rights. They also do not impose

277 MD. CODE ANN., HEALTH–GEN. § 13-2002(a) (West 2019).
278 45 C.F.R. § 46.111(a)(7) (2018).
279 N.J. STAT. ANN. § 26:14-4 (West 2019).
280 VA. CODE ANN. §§ 32.1-162.18(C), .19–.20 (West 2019).
281 N.Y. PUB. HEALTH LAW §§ 2440–2446 (McKinney 2019).
282 CAL. HEALTH & SAFETY CODE §§ 24170–24178 (West 2019).
283 *Id.* § 24174.

administrative requirements on regulated persons and entities that would support compliance with any use and disclosure requirements or individual rights. Two states do, however, have relatively robust data privacy laws that are potentially applicable to mobile-app-mediated research conducted by independent scientists. In particular, Texas has a data privacy law that is a slimmed-down version of the HIPAA Privacy Rule.[284] California has a data privacy law modeled after the GDPR that goes into effect January 1, 2020.[285] The Texas and California laws should be considered by state policymakers wishing to address the privacy concerns raised by mobile research apps.

At the outset, it is important to note that the Texas law is codified in the state's Health and Safety Code and is named the Texas Medical Records Privacy Act, which suggests (at least original) intent as a health industry law.[286] On the other hand, the California Consumer Privacy Act of 2018 is codified outside the California Health and Safety Code—in the California Civil Code instead—suggesting a broader, consumer-oriented intent.[287] The Texas law thus may be viewed (at least originally) as an intra- (health-) industry law, whereas the California Act may be viewed as an inter- (or cross-) industry law. It is no surprise that the content of the Texas law is modeled after the HIPAA Privacy Rule, which is understood as a health industry law, whereas the California Act is modeled after the GDPR, which is known as an interindustry law.

The Texas law has extremely broad application. The Texas law applies to a "covered entity," defined as any person who

> (A) for commercial, financial, or professional gain, monetary fees, or dues, or on a cooperative, nonprofit, or pro bono basis, engages, in whole or in part, and with real or constructive knowledge, in the practice of assembling, collecting, analyzing, using, evaluating, storing, or transmitting protected health information. The term includes a business associate, health care payer, governmental unit, information or computer management entity, school, health researcher, health care facility, clinic, health care provider, or person who maintains an Internet site;
>
> (B) comes into possession of protected health information; [or]
>
> (C) obtains or stores protected health information . . . .[288]

Mobile-app-mediated health researchers would constitute health researchers under the first clause of the definition. They would also come into possession of protected health information under the second, alternate clause of the definition. The Texas law, as written and without any necessary amendments, would thus regulate all mobile-app-mediated health researchers.

284 *See* TEX. HEALTH & SAFETY CODE ANN. §§ 181.001–.207 (West 2019).

285 *See* California Consumer Privacy Act of 2018, 2018 Cal. Legis. Serv. ch. 55, A.B. 375 (West) (to be codified at CAL. CIV. CODE §§ 1798.100–.198) (effective Jan. 1, 2020), *amended by* 2018 Cal. Legis. Serv. ch. 735, S.B. 1121 (West).

286 *See* TEX. HEALTH & SAFETY CODE ANN. §§ 181.001–.207 (West 2019).

287 *See* California Consumer Privacy Act of 2018 (to be codified at CAL. CIV. CODE §§ 1798.100–.198).

288 TEX. HEALTH & SAFETY CODE ANN. § 181.001(b)(2)(A)–(C) (West 2019).

Note that mobile-app developers as well as backend data storage companies, which frequently obtain or store protected health information from or for mobile-app-mediated researchers,[289] would also fit into the second and third alternate clauses of the definition of covered entity. For these reasons, this Article strongly recommends the Texas definition of covered entity.

The Texas law contains a number of important privacy provisions that are the same as, or similar to, the use and disclosure requirements, the individual rights, and the administrative requirements set forth in the HIPAA Privacy Rule. That is, the Texas law requires covered entities to (1) provide notice to any individual whose protected health information will be electronically disclosed by the covered entity; (2) not electronically disclose an individual's protected health information without a separate, prior authorization from the individual; (3) not disclose an individual's protected health information in exchange for direct or indirect remuneration; (4) obtain a clear and unambiguous permission in written or electronic form before using or disclosing an individual's protected health information for marketing purposes; and (5) train their employees regarding their data privacy responsibilities.[290] The Texas Attorney General, who has the authority to seek injunctive relief and to impose civil penalties for violations of the law, actively enforces the law.[291]

At this point, it may be helpful to review the hypothetical that opened this Article to see how comprehensive and applicable Texas's privacy law is. In the hypothetical that opened this Article, a woman with a progressive neurological condition, who wished to advance the scientific understanding of her disease, volunteered to participate in a disease progression research study led by an independent scientist. The study required the woman to download and use a mobile app that was designed by the independent scientist and that collected a number of data elements, including first and last name, date of birth, race, ethnicity, diagnosis, medications, family history, and real-time information regarding balance, gait, vision, cognition, and other measures of disease progression.

During the research study, remember that the independent scientist electronically disclosed the woman's identifiable data to other researchers worldwide without the woman's prior notification or authorization. However, the Texas law would have prohibited both the electronic disclosure and the lack of prior notification to the woman of the disclosure. Remember that the independent scientist also sold the woman's name, address, and diagnosis to a healthcare marketing company. However, the Texas law would have prohibited this sale of identifiable health information. The hypothetical also

289 *See* Moore et al., *supra* note 3 (providing data regarding mobile-app-mediated researchers who use third-party, backend data collection and/or storage companies).

290 TEX. HEALTH & SAFETY CODE ANN. §§ 181.101, .152–.154 (West 2019).

291 *Id.* § 181.201; *see also* OFFICE OF THE TEX. ATTORNEY GEN., TEXAS MEDICAL RECORDS PRIVACY ACT ANNUAL REPORT: FISCAL YEAR 2016, at 3–4 (2016) (summarizing the Texas Attorney General's substantial enforcement activities relating to the Texas Medical Records Privacy Act).

involved a hacker who accessed the woman's data as the data traveled from the woman's smart phone to the scientist's contracted backend data collector. Remember that the scientist neither notified the woman of this security breach nor provided her with instructions regarding how to minimize her potential economic, dignitary, and psychological injuries associated with the breach. However, Texas's breach notification law, which applies to any "person,"[292] would have required the scientist to follow a number of important and helpful breach notification procedures. In summary, Texas has comprehensive privacy, security, and breach notification provisions that, if complied with, would have prevented the woman's informational injuries or helped to minimize such injuries. One important finding of this Article, then, is that states like Texas have the current infrastructure necessary to address the privacy- and security-related concerns raised by independent, mobile-app-mediated health research.

Now let us turn to California, the second state with a relatively comprehensive and potentially applicable data privacy statute. In late June 2018, then-Governor Jerry Brown signed into law the California Consumer Privacy Act of 2018.[293] To be codified in the state's Civil Code, the Act will become effective January 1, 2020.[294] The Act's legislative history details the many reasons for the legislation, including the increase in the amount of personal information, including health information, shared by California consumers and the need to give California consumers control over the collection, use, and disclosure of their personal information.[295]

One catch with the California Act is that it does not apply to anyone who comes into possession of, or anyone who stores or collects, identifiable health information like the Texas law does. The California Act only applies to a business, defined as a sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners, that (1) collects consumers' personal information and determines the purposes and means of processing of consumer information; (2) does business in California; and (3) satisfies one or more of the following thresholds: (a) has annual gross revenues in excess of $25 million; (b) annually buys, receives, sells, or shares for commercial purposes the personal information of 50,000 or more consumers or households; or (c) derives fifty percent or more of its annual revenues from selling consumers' personal information.[296]

A postenactment amendment (SB 1121, signed into law on September 23, 2018), clarifies that the California Act does not protect data obtained

292 TEX. BUS. & COM. CODE ANN. § 521.053 (West 2019).

293 *See* 2018 Cal. Legis. Serv. ch. 55, A.B. 375 (West) (to be codified at CAL. CIV. CODE §§ 1798.100–.198) (effective Jan. 1, 2020), *amended by* 2018 Cal. Legis. Serv. ch. 735, S.B. 1121 (West).

294 *Id.*

295 *Id.*

296 *Id.*

during clinical trials.[297] In addition, many independent scientists may not reach the financial thresholds set forth in the law; that is, they may not have gross annual revenues in excess of $25 million; they may never conduct a research project that uses the data of 50,000 or more research participants; and they may not derive fifty percent or more of their revenues from selling consumers' personal information. For these reasons, this Article does not recommend that other states use the California Act—at least its application provision—as a model.

Once the California Act applies, however, it broadly protects personal information, defined to include medical information, geolocation data, and a wide variety of behaviors, preferences, and trends, which are frequently collected by mobile research apps and other big data capture tools. In addition, the Act gives consumers a number of information rights that are the same as, or similar to, the rights set forth in the GDPR. These include, but are not limited to, the rights to (1) request that a business that collects a consumer's personal information disclose to that consumer the categories and specific pieces of personal information the business has collected, the business or commercial purpose for collecting or selling the personal information, and the categories of third parties with whom the business discloses personal information; (2) direct a business that sells personal information about the consumer to third parties not to sell the consumer's personal information (the right to "opt out"); (3) not have businesses collect additional categories of personal information or use existing categories of personal information beyond that agreed upon in a required notice of information practices; (4) request that a business delete any personal information about the consumer that the business has collected from the consumer; and (5) not be discriminated against because the consumer has exercised any of the consumer's rights under the Act.[298] In terms of administrative requirements, the Act requires a business, in a form that is reasonably accessible to consumers, to provide a web or online link that a consumer can click on to opt out of the sale of the consumer's information.[299] The Act thus places the burden on the consumer to opt out of the sale of the consumer's personal information, whereas Texas law contains an outright prohibition on the sale of a consumer's health information.[300] Other than its somewhat narrow application provision, the California Act could serve as a model for other states looking to adopt cross-industry privacy protections that are designed to keep pace with big data.

---

297 2018 Cal. Legis. Serv. ch. 735, S.B. 1121, § 10(c)(1)(C) (amending CAL. CIV. CODE § 1798.145).

298 *See* 2018 Cal. Legis. Serv. ch. 55, A.B. 375.

299 *Id.*

300 *Compare* 2018 Cal. Legis. Serv. ch. 735, S.B. 1121, § 10(c)(1)(C) *and* 2018 Cal. Legis. Serv. ch. 55, A.B. 375, *with* TEX. HEALTH & SAFETY CODE ANN. §§ 181.101, .152–.154 (West 2019).

Conclusion and Proposals

This Article has carefully discussed whether nonsectoral state statutes may serve as a viable source of privacy and security protections for mobile health research participants and other health-related big-data subjects. In particular, this Article has catalogued and analyzed all potentially applicable, nonsectoral, data privacy, security, and breach notification statutes set forth in the laws of all fifty states and the District of Columbia. Contrary to prior assumptions regarding the capacity of state law in this area, this Article has found that all states have potentially applicable breach notification statutes and that each of these statutes contains individual breach notification provisions designed to put data subjects on notice of security breaches. This Article has also shown that, depending on the circumstances of the breach, approximately three-fifths of states require notification to a state agency or the state police, approximately two-thirds of states require notification to consumer reporting agencies, and more than ninety percent of states require a third-party agent, data storage company, data processor, data nonowner, or data nonlicensee to notify the data controller, data owner, or data licensee of a security breach.

This Article has further shown that most state breach notification statutes could be used to protect mobile research participant data with four minor changes. First, state statutes that currently regulate only government agencies, large corporations, and other institutions could be amended to regulate natural persons as well. Second, state statutes that require the regulated person or entity to be doing business in the state could be amended to clarify that owning and using personal data of a state resident constitutes doing business in that state. Third, state statutes that currently require the first name or first initial and last name of a data subject to be present before data will be protected could be amended to allow other identifiers to be present as well, thus responding to the increasing ability to reidentify individuals with nonobvious identifiers. Fourth, state statutes that currently protect only social security numbers, driver's license numbers, state identification card numbers, financial account numbers, and credit or debit card numbers could be amended to protect physical and mental health data and other behaviors, preferences, and trends as well. These amendments would create cross-industry breach notification protections that would benefit more health data subjects (including mobile health research participants) from all informational injuries, not just economic injuries associated with traditional identity theft.

This Article has found that fewer states have potentially applicable security and privacy statutes. In particular, approximately two-thirds of states have at least one potentially applicable data security statute. These security provisions tend to be extremely modest when compared to federal and international industry standards. For example, they briefly address the secure disposal of data but fail to address the security of maintained, or nondisposed, data. Those states that extend security requirements to nondisposed data tend to require "appropriate and reasonable safeguards" but fail to spec-

ify what those safeguards should be and when they would be considered appropriate or reasonable. That said, a handful of states, including Ohio, Oregon, and Massachusetts, do have comprehensive security laws, and this Article recommends the use of these security laws as a guide for other states.

Finally, approximately one-quarter of states have at least one data privacy statute that is potentially applicable to independent scientists who conduct mobile-app-mediated research. These statutes include modest online privacy policy laws, privacy policy false statement laws, notice of intent to sell nonpublic personal information laws, and human research laws. However, Texas and California have robust data privacy laws that should be considered, in whole or in part, by other states for use in protecting against informational injuries associated with mobile-app-mediated health research.

* * *

Although sectoral approaches to privacy and security made sense as late as a quarter of a century ago, when most data originated in the industry to which it pertained, the time has come for generally applicable forms of data protection. Traditional, intraindustry approaches to privacy and security regulation certainly have some benefits. One is regulator familiarity with the information practices of the regulated entity. For example, state medical boards, which are composed of state-licensed physicians, are very familiar with the information practices of other state-licensed physicians, whom they regulate. The HHS, by further example, is familiar with the information practices of healthcare providers that electronically submit claims to HHS programs, including Medicare and Medicaid.

It is not clear, however, that regulator comfort and other benefits of intraindustry regulation continue to outweigh the risks of limited regulatory authority. Today, health data is generated not only by traditional members of the healthcare industry, including healthcare providers, health plans, and healthcare clearinghouses, but also by independent scientists as well as a range of other individuals and institutions, including data subjects themselves. The significant economic, dignitary, and psychological harms associated with health data breaches and the lack of applicable federal regulations suggest a need for comprehensive and generally applicable privacy, security, and breach notification regulation.

In light of the findings presented in this Article, policymakers should consider nonsectoral state statutes as a possible option for protecting health data if generally applicable, federal data laws are not enacted or enforced. Because all fifty-one jurisdictions have data breach notification statutes, and more than two-thirds have nearby security statutes, one option for states is to (1) amend existing breach notification statutes in accordance with the guidelines set forth in this Article and (2) use the security statutes of Ohio, Oregon, and Massachusetts and the privacy laws of Texas and California as a guide for new security and privacy legislation. From an academic (and optics) standpoint, the security and privacy content should be codified near, but before, the breach notification content. That is, it is the development

and implementation of privacy and security standards that minimizes the risk of privacy and security breaches.

A second option is for the National Conference of Commissioners on Uniform State Laws to take the substantive recommendations set forth in this Article and to draft a uniform data privacy, security, and breach notification law that could be adopted or considered by all jurisdictions. Because many mobile-app-mediated researchers will collect research data from participants located in more than one state, this option has the benefit of creating uniformity among state laws, which would greatly ease individual and institutional compliance efforts.[301] Regardless of the path ultimately followed, regulation is quickly needed to address the rapidly growing privacy and security concerns raised by big data, including mobile-app-mediated health research.

301 *See, e.g.*, Elliott T. Dube, *Patchwork Privacy Laws Stifle Medical Studies Across State Lines*, Bloomberg L. (May 28, 2019), https://news.bloomberglaw.com/pharma-and-life-sciences/patchwork-privacy-laws-stifle-medical-studies-across-state-lines-1 ("Abiding by a patchwork of laws during multi-state clinical trials will be expensive and time consuming and slow progress in research and new treatments.").