Mobile Research Applications and State Data Protection Statutes

Stacey A. Tovino

Introduction

This article focuses on state privacy, security, and data breach regulation of mobile-app mediated health research, concentrating in particular on research studies conducted or participated in by independent scientists, citizen scientists, and patient researchers. Prior scholarship addressing these issues tends to focus on the lack of application of the HIPAA Privacy and Security Rules and other sources of federal regulation.[1] One article, however, mentions state law as a possible source of privacy and security protections for individuals in the particular context of mobile app-mediated health research.[2] This article builds on this prior scholarship by: (1) assessing state data protection statutes that are potentially applicable to mobile app-mediated health researchers; and (2) suggesting statutory amendments that could better protect the privacy and security of mobile health research data. As discussed in more detail below, all fifty states and the District of Columbia have potentially applicable data breach notification statutes that require the notification of data subjects of certain informational breaches in certain contexts. In addition, more than two-thirds of jurisdictions have potentially applicable data security statutes and almost one-third of jurisdictions have potentially applicable data privacy statutes. Because all jurisdictions have data breach notification statutes, these statutes will be assessed first.

Data Breach Notification Laws

All fifty-one jurisdictions have data breach notification statutes that are potentially applicable to independent scientists, citizen scientists, and patient researchers who conduct or participate in mobile app-mediated health research.[3] The statutes are "potentially applicable" because they are not limited in application to certain licensed professionals, such as physicians or nurses; certain institutions, such as hospitals or academic medical centers; or certain transactions or sources of funding, such as insurance claims or federal funding. By definition, the independent scientists, citizen scientists, and patient researchers who are the focus of this article are not licensed health care professionals. They are not employed by hospitals, government agencies, or other institutions, and they do not receive federal funding.

All fifty-one of these data 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 circumstances of the breach.[4] Forty-eight (94.1%) of the breach notification statutes require a third-party agent, data storage company, data processor, data non-owner, or data non-licensee to notify the appropriate regulated entity, data controller, data owner, or data licensee of the breach, depending on the circumstances of the breach.[5] Thirty-four (66.7%) of the breach notification statutes require notification of consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, depending on the circumstances of the breach.[6] Thirty (58.8%) of the breach notification statutes also require notification of the state Attorney General, state Department of Legal Affairs, state Office of Consumer Protection, and/or state police, depending on the circumstances of the breach.[7] These statutes are extremely valuable in the context of mobile research applications because,

Stacey A. Tovino, J.D., Ph.D., *is the Judge Jack and Lulu Lehman Professor of Law at the William S. Boyd School of Law, University of Nevada-Las Vegas.*

The Journal of Law, Medicine & Ethics, 48 S1 (2020): 87-93. © 2020 The Author(s)
DOI: 10.1177/1073110520917033

if applicable, they would alert a research participant of a data breach and notify the participant how to take protective measures.

Moving from content to application, these statutes tend to have broad, but not unlimited, application. For example, Alabama's data breach notification statute applies to a covered entity, defined 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."[8] The Alabama statute 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.

To remove questions regarding applicability to mobile app-mediated research studies conducted by independent scientists, citizen scientists, and patient researchers, states may wish to consider statutory amendments that would regulate all natural or legal persons who collect, assemble, evaluate, or transfer personal information regardless of whether remuneration is involved.

An independent scientist certainly is a person and could also be a sole proprietorship, thus meeting the first part of the Alabama statute's definition of covered entity. Depending on the mobile app-mediated research project, however, the scientist may not be acquiring or using sensitive personally identifying information as necessary for regulation to occur. For example, some mobile research apps collect neither the name (nor any type of user identity) nor precise geolocation of their citizen scientists.[9] However, these apps may collect data regarding the city, state, and country (e.g., "Seminole, Florida, USA") where health symptoms or concerns occurred, as well as the age, gender, and IP address of the reporting citizen sex scientist. Because the Alabama law only protects information tied to the first name or first initial and last name of a data subject, the Alabama statute — as currently written — does not regulate some mobile research apps.

Approximately three dozen other data breach notification laws share this limitation and only protect data 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.[10] These data breach notification statutes 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."[11] Stated another way, these breach notification statutes have not kept up with Big Data's ability to re-identify individuals with non-obvious identifiers. States that protect data only when tied to the first name or first initial and last name of the data subject may wish to consider expanding the category of protected data.

Other data breach notification statutes, however, contain slightly broader definitions of protected data. Montana's data breach notification statute, for example, defines personal information as "an individual's name, signature, address, or telephone number" in combination with other information, thus recognizing that an individual's signature, address, or telephone number could also be used to identify an individual.[12] In counties with publicly accessible property records, 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. The Montana statute recognizes this fact, thus including address in its definition of personal information. Texas's data breach notification statute, by further example, allows an individual's first name or first initial and last name in combination with other data to constitute "sensitive personal information."[13] However, Texas's statute also protects other "information that identifies the individual and relates to the physical or mental health or condition of the individual." States with limited definitions of protected data may wish to consider expanding those definitions in accordance with the Montana or Texas statutes.

Still other limitations in state data breach notification statutes become apparent when applied to independent scientists who conduct mobile app-mediated research. Georgia's statute for example, applies to "data collectors" and "information brokers."[14] "Data collectors" are defined as are state and local agencies. "Information brokers" are persons who, for monetary fees or dues, engage in collecting, assembling, evaluating, and transferring information concerning individuals. By definition, an independent scientist does not work for

The Journal of Law, Medicine & Ethics, 48 S1 (2020): 87-93. © 2020 The Author(s)

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, although some mobile applications' privacy policies state that collected data are sold to third parties for research purposes. To remove questions regarding applicability to mobile app-mediated research studies conducted by independent scientists, citizen scientists, and patient researchers, states may wish to consider statutory amendments that would regulate all natural or legal persons who collect, assemble, evaluate, or transfer personal information regardless of whether remuneration is involved.

Still other data breach notification statutes require a person or entity to be "doing business" or "conducting business" in the state before regulation occurs. New Hampshire's statute, for example, applies to "any person doing business in New Hampshire."[15] 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 information owning or using does not have a physical presence in the state.[16] These statutes are desirable in terms of protecting mobile research data because the researcher may be physically located in one state, but the app may collect data from residents of all states. Other state statutes fail to clarify whether the collection and use of data regarding a state resident (without more) constitutes "doing business" or "conducting business." States with unclear language may wish to consider statutory amendments that expressly include collecting and using data of residents within the definition of "doing business" or "conducting business."

More broadly, some state breach notification statutes apply to government agencies, private corporations, and other types of legal persons, but not natural persons. Illinois's statute, 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, and any other business entity that, for any purpose, handles, collects, disseminates, or otherwise deals with nonpublic personal information.[17] Other state statutes, however, specifically apply to natural persons and sole proprietorships.[18] Given that many independent scientists, citizen scientists, and patient researchers are unincorporated and/or work alone, states may wish to consider including natural persons and sole proprietorships as well as larger organizations in their list of regulated entities.

Finally, most breach notification statutes appear not to have contemplated the collection of data by mobile application. However, Illinois's Personal Information Protection Act defines protected "medical information" to include information regarding an individual's physical or mental health condition, including information "provided to a … mobile application."[19] Given the growing use of mobile apps for health and research purposes, states may wish to clarify that protected data includes data provided to a mobile application.

Data Security Statutes

At least two-thirds of jurisdictions have at least one potentially applicable data security statute.[20] In some cases, the persons and entities regulated by the state's security statute are the same as those regulated by the state's breach notification statutes.[21] In other cases, the persons and entities regulated by the state's security statute are different than those regulated by the state's breach notification statute.[22] In either case, the issues identified above regarding the persons and entities regulated by state breach notification statutes also apply to the persons and entities regulated by state security statutes. For example, a state security statute that only applies to a government agency or a public corporation could be amended to apply to a natural person and a sole proprietorship, which could include an independent scientist or citizen scientist. By further example, a state security statute that only applies to a person or entity doing business in the state could be amended to clarify that owning or using personal data of a state resident constitutes doing business in the state.

Many of the state data security statutes are quite limited. For example, the Alaska security statute 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."[23] Far from a comprehensive security law, the Alaska security statute may be properly classified as a "secure disposal" or "secure destruction" law. That is, the Alaska statute does not mandate any administrative, technical, or physical safeguards outside the context of the disposal or destruction of personal information. The Alaska statute does not address, for example, the need for security policies and procedures addressing non-disposed data; the designation of a data security officer to oversee implementation of and compliance with such policies and procedures with respect to non-disposed data; encryption; access controls; or identifying and responding to suspected or known security incidents involving non-disposed data.

In contrast, 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 physi-

The Journal of Law, Medicine & Ethics, 48 S1 (2020): 87-93. © 2020 The Author(s)

cal safeguards that must be adopted.[24] Massachusetts law delegates to a state agency the duty to promulgate comprehensive security standards, a task the agency completed by its stated deadline.[25] Ohio has a Cybersecurity Act that provides 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.[26] Given the importance of comprehensive security protections for mobile research data and other sensitive and potentially stigmatizing personal data, states with modest secure disposal statutes should consider expanding their statutes, using the Oregon, Massachusetts, or Ohio statutes as a guide.

Data Privacy Statutes

A review of state statutes reveals a wide range of approaches—some modest and some comprehensive—to data privacy. For example, some states merely require operators of online services to create and post data privacy policies.[27] Other states simply forbid false or misleading statements in online privacy policies.[28] Still other limited state statutes require certain persons to provide certain consumers with a notice of intent to sell their nonpublic personal information before selling their nonpublic personal information.[29] A growing number of states, however, are considering enacting, or have recently enacted, comprehensive data privacy legislation.[30] Although a review of all approaches to state data privacy are beyond the scope of this Article, two examples of comprehensive data privacy legislation, Texas and California, are provided below.

Enacted in 2001, the Texas Medical Records Privacy Act (TMRPA) has extremely broad application,[31] covering any person who: (1) "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"; (2) "comes into possession of protected health information"; or (3) "obtains or stores protected health information." Mobile app-mediated health researchers would constitute health researchers under the first clause of the definition. These researchers also may come into possession of protected health information under the second, alternate clause of the definition. A desirable feature of the TMRPA is that it excepts HIPAA covered entities from state regulation and directs such entities to comply with the HIPAA Privacy Rule, thus avoiding conflicts of laws questions for traditional researchers affiliated with HIPAA-covered academic medical centers.

The TMRPA currently regulates many mobile app-mediated health researchers. Note that mobile application developers as well as back-end data storage companies, which frequently obtain or store protected health information for or on behalf of mobile device-mediated researchers, would also fit into the second and third alternate clauses of the definition of covered entity under the TMRPA. States considering enacting comprehensive data privacy legislation should consider the TMRPA's definition of covered entity.

The TMRPA contains a number of important data privacy provisions, such as requiring 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. The Texas Attorney General, who has authority to seek injunctive relief and to impose civil penalties for violations of the TMRPA, actively enforces the law.[32]

The California Consumer Privacy Act (CCPA)[33] is a second example of a comprehensive state data privacy statute that has potential relevance to mobile app-mediated health researchers. One limitation of the CCPA is that it does not apply to anyone who comes into possession of, or anyone who stores or collects, identifiable health information, like the TMRPA. The CCPA 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

The Journal of Law, Medicine & Ethics, 48 S1 (2020): 87-93. © 2020 The Author(s)

or more of its annual revenues from selling consumers' personal information.

The CCPA thus does not expressly apply to natural persons, which many independent scientists, citizen scientists, and patient researchers are. A post-enactment amendment further clarifies that the CCPA does not protect data obtained during clinical trials.[34] 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, other states considering enacting comprehensive data privacy legislation may wish to avoid using the CCPA's application provisions as a guide.

Because many mobile app-mediated research projects collect data from participants who reside in different states, uniformity of state privacy, security, and data breach notification statutes will be key to compliance, investigation, and enforcement.

Once the CCPA applies, however, the statute broadly protects "personal information," defined as information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. The CCPA includes a generous, illustrative list of items that fall within the definition of personal information, including names, physical addresses, email addresses, internet protocol addresses, geolocation data, social security numbers, telephone numbers, driver's license numbers, account numbers, biometric identifiers, physical descriptions, medical information, insurance information, financial information, employment information, purchase histories, and browser histories, as well as inferences that can be drawn from the preceding items regarding consumer preferences, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes. A post-enactment amendment to the CCPA[35] clarifies, however, that personal information does not include consumer information that is "deidentified"[36] "or aggregate consumer information."[37] Given the increasing ability of data aggregators to identify or reidentify data subjects using non-obvious identifiers,[38] the application of these definitions will be critical in determining whether the CCPA protects California resident data collected by mobile research apps.

The CCPA gives California residents several important privacy rights with respect to their personal information, including: (1) the right to be informed of the categories of personal information that are being collected and the purposes for which such information shall be used, (2) the right not to have additional personal information collected without further notice, (3) the right to request deletion of personal information, (4) the right to know whether personal information is being sold or disclosed and to whom, (5) the right to opt out of the sale of personal information, (6) the right to access personal information, and (7) the right to equal services and prices regardless of whether privacy rights under the CCPA are exercised. In certain cases involving unauthorized access to, or theft or disclosure of, certain categories of personal information, as well as in certain cases involving other violations, the CCPA provides for civil damages, civil penalties, injunctive or declaratory relief, and other relief that a court may deem proper.[39] Other than its somewhat narrow application provision, which requires the meeting of certain financial thresholds by a business, the CCPA provides a model for other states looking to adopt data privacy protections designed to keep pace with mobile and other technologies.

Conclusion

This article has assessed state privacy, security, and data breach notification statutes in the context of concerns raised by mobile app-mediated health research and has suggested statutory amendments that would help protect mobile research data. Because many mobile app-mediated research projects collect data from participants who reside in different states, uniformity of state privacy, security, and data breach notification statutes will be key to compliance, investigation, and enforcement. To promote uniformity in state laws, organizations that draft and advocate for the adoption of uniform or model state laws, such as the Uniform Law Commission (ULC), are encouraged to initiate efforts to draft uniform data protection laws.

Acknowledgments

Research on this article was funded by the following grant: Addressing ELSI Issues in Unregulated Health Research Using Mobile Devices, No. 1R01CA20738-01A1, National Cancer Institute, National Human Genome Research Institute, and Office of Science Policy and Office of Behavioral and Social Sciences Research

The Journal of Law, Medicine & Ethics, 48 S1 (2020): 87-93. © 2020 The Author(s)

https://doi.org/10.1177/1073110520917033 Published online by Cambridge University Press

in the Office of the Director, National Institutes of Health, Mark A. Rothstein and John T. Wilbanks, Principal Investigators.

Note

The author has no conflicts of interest to disclose.

References

1. *See*, e.g., G. Cohen and M. Mello, "HIPAA and Protecting Health Information in the 21st Century," *JAMA Online First*, May 24, 2018 ("The reality … is that HIPAA-covered data form a small and diminishing share of the health information stored and traded in cyberspace."); N.P. Terry and T.D. Gunter, "Regulating Mobile Mental Health Apps," *Behavioral Sciences and the Law* 36, no. 1 (2018): 136-144 ("[Mobile medical applications] tend to be developed outside of traditional health care spaces with the result that they exist in a lightly regulated, 'HIPAA-free zone.'"); M.A. Rothstein, J.T. Wilbanks, and K.B. Brothers, "Citizen Science on Your Smartphone: An ELSI Research Agenda," *Journal of Law, Medicine & Ethics* 43, no. 4 (2015): 897-903 ("[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.").
2. *See* Rothstein, Wilbanks and Brothers, *supra* note 1, at 899 (referencing states that extend research protections to non-federally supported research but noting that these laws "do not provide significant protections or remedies in the event of breaches of research or privacy standards").
3. *See* Ala. Code § 8-19F (hereinafter Alabama); Alaska Stat. § 45.48 (hereinafter Alaska); Ariz. Rev. Stat. §§ 18-551 – 552 and Ariz. Rev. Stat. § 44-7601 (hereinafter Arizona); Ark. Code § 4-110 (hereinafter Arkansas); Cal. Civ. Code §§ 1798.1-.82 and Cal. Civ. Code §§ 1789.100-.198 (hereinafter California); Colo. Rev. Stat. §§ 6-1-713 - 716 (hereinafter Colorado); Conn. Gen. Stat. §§ 36a-701a-b and Conn. Gen. Stat. § 42-471 (hereinafter Connecticut); Del. Code tit. 6, Chapter 12B-100 – 104 and Del. Code tit. 6, § 5001C (hereinafter Delaware); D.C. Code §§ 28-3851—28-3853 (hereinafter District of Columbia); Fla. Stat. § 501.171 (hereinafter Florida); Ga. Code §§ 10-1-910 – 912 and Ga. Code § 10-15-2 (hereinafter Georgia); Haw. Rev. Stat. §§ 487N-1 – N3 and Haw. Rev. Stat. § 487R-2 (hereinafter Hawaii); Idaho Code §§ 28-51-104—107 (hereinafter Idaho); 815 ILCS §§ 530/1—50 (hereinafter Illinois); Ind. Code § 24-4.9 (hereinafter Indiana); Iowa Code §§ 715C.1—.2 (hereinafter Iowa); Kan. Stat. Ann. § 50-7a01—04 and Kan. Stat. Ann. § 50-6,139b (hereinafter Kansas); Ky. Rev. Stat. §§ 365.720—.734 (hereinafter Kentucky); La. Rev. Stat. §§ 51:3071-3074 (hereinafter Louisiana); Me. Rev. Stat. Ann. tit. 10 §§ 1346—1350-B (hereinafter Maine); Md. Code Com. Law §§ 14-3501—14-3508 (hereinafter Maryland); Mass. Gen. Laws §§ 93H-1-6 and 201 CMR §§ 17.01 - 17.05 (hereinafter Massachusetts); Mich. Comp. Laws §§ 445.63—79d (hereinafter Michigan); Minn. Stat. Ann. § 325E.61 (hereinafter Minnesota); Miss. Code § 75-24-29 (hereinafter Mississippi); Mo. Rev. Stat. § 407.1500 (hereinafter Missouri); Mont. Code Ann. §§ 30-14-1701—1736 (hereinafter Montana); Neb. Rev. Stat. §§ 87-801-808 (hereinafter Nebraska); Nev. Rev. Stat. §§ 603A.010.—.920 (hereinafter Nevada); N.H. Rev. Stat. §§ 359-C:19—21 (hereinafter New Hampshire); N.J. Stat. §§ 56:8-161—163 (hereinafter New Jersey); N.M. Stat. Ann. §§ 57-12c-1—12 (hereinafter New Mexico); N.Y. Gen. Bus. Law § 899-AA and N.Y. Gen. Bus. Law § 399-h (hereinafter New York); N.C. Gen. Stat. §§ 75-60—66 (hereinafter North Carolina); N.D. Cent. Code §§ 51-30-01—51-30-07 (hereinafter North Dakota); Ohio Rev. Code §§ 1349.19, 1349.191, 1349.192 and Ohio Rev. Code Ann. § 1354.01 (hereinafter Ohio); Okla. Stat. tit. 24 §§ 161—166 (hereinafter Oklahoma); Or. Reg. Stat. Ann. §§ 646A.600—.628 (hereinafter Oregon); 73 Pa. Stat. §§ 2301—2309 (hereinafter Pennsylvania); R.I. Gen. Laws §§ 11-49.3-1—6 and R.I. Gen. Laws § 6-52-2 (hereinafter Rhode Island); S.C. Code § 39-1-90 (hereinafter South Carolina); S.D. Cod. Laws §§ 22-40-19—26 (hereinafter South Dakota); Tenn. Code §§ 47-18-2101—2111 and Tenn. Code § 39-14-150(g) (hereinafter Tennessee); Tex. Bus. & Com. Code §§ 521.002, 521.053 (hereinafter Texas); Utah Code § 13-44-101—301 (hereinafter Utah); Vt. Stat. tit. 9 §§ 2430—2445 (hereinafter Vermont); Va. Code § 18.2-186.6 (hereinafter Virginia); Wash. Rev. Code § 19.255.010 and Wash. Rev. Code § 19.215.020 (hereinafter Washington); W.Va. Code §§ 46A-2A-101—105 (hereinafter West Virginia); Wis. Stat. Ann. §§ 134.97-98 (hereinafter Wisconsin) Wyo. Stat. §§ 40-12-501—40-12-509 (hereinafter Wyoming). *See generally* S.A. Tovino, "Going Rogue: Mobile Research Applications and the Right to Privacy," *Notre Dame Law Review* 95, no. 1 (2019): 155-209 (thoroughly discussing state data breach, data security, and data privacy statutes potentially applicable to mobile app-mediated research studies conducted by independent scientists, citizen scientists, and patient researchers).
4. *See supra* note 1 (at all jurisdictions listed).
5. *See id.* (at all jurisdictions except Alaska, Rhode Island, and South Dakota).
6. *See id.* (at Alabama, Alaska, Arizona, Colorado, District of Columbia, Florida, Georgia, Hawaii, Indiana, Kansas, Kentucky, 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, and Wisconsin).
7. *See id.* (at Alabama, Arizona, California, Colorado, Connecticut, Delaware, Florida, Hawaii, Idaho, Indiana, Iowa, Maine, Maryland, Massachusetts, Missouri, Montana, Nebraska, New Hampshire, New Jersey, New Mexico, New York, North Carolina, North Dakota, Oregon, Rhode Island, South Carolina, South Dakota, Vermont, Virginia, and Washington).
8. *See* Ala. Code § 8-19F-2.
9. For example, the Kinsey Reporter mobile app collects real-time, reportedly anonymous data about sexual health, sexual behaviors, and other intimate behaviors reported by their citizen sex scientists. Kinsey Reporter communicates the collected data to Kinsey Reporter.org, a global mobile platform designed by researchers based in Bloomington, Indiana, that aggregates, maps, and shares reportedly anonymous data with the public. *See* Apple App Store, Kinsey Reporter; GooglePlay, Kinsey Reporter.
10. *See supra* note 3 (at Alaska, Arkansas, Colorado, Connecticut, Delaware, District of Columbia, Hawaii, Idaho, Indiana (also allowing 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).
11. *See, e.g.*, C.F. Kerry, "Why Protecting Privacy Is a Losing Game Today — And How to Change the Game," *Brookings*, July 12, 2018 ("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 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.").
12. *See* Mont. Code Ann. § 30-14-1702.
13. *See* Tex. Bus. & Com. Code § 521.002.
14. *See* Ga. Code § 10-1-912.
15. *See* N.H. Rev. Stat. § 359-C:20.
16. *See* Ind. Code § 24-4.9-2-4.
17. *See* 815 ILCS § 530/10.

The Journal of Law, Medicine & Ethics, 48 S1 (2020): 87-93. © 2020 The Author(s)

18. *See, e.g.*, Ind. Code § 24-4.9-2-3 (defining person as an individual as well as a corporation).
19. *See* 815 ILCS § 530/5 (defining "personal information," which internally references the definition of "medical information").
20. *See supra* note 3 (at Alabama, Alaska, Arizona, Arkansas, California, Colorado, Connecticut, Delaware, Florida, Georgia, Hawaii, Illinois, Indiana, Kansas, Kentucky, Louisiana, 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).
21. *See, e.g.*, Ark. Code § 4-110-104 (setting forth a modest security law that applies to persons and businesses, which are also regulated by Arkansas' breach notification law).
22. *See, e.g.*, Alaska Stat. §§ 45.48.500 (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).
23. *Id.* § 45.48.510.
24. *See* Or. Rev. Stat. Ann. § 646A.622.
25. *See* Mass. Gen. Laws § 93H-2; 201 Code Mass. Regs. §§ 17.01-17.05.
26. *See* Ohio Rev. Code Ann. §§ 1354.01-.02.
27. *See, e.g.*, Cal. Bus. & Prof. Code §§ 22575-22579.
28. *See, e.g.*, Neb. Rev. Stat. § 87-302(15); Or. Rev. Stat. § 646.607(12); 18 Pa. Cons. Stat. Ann. § 4107(a)(10).
29. *See, e.g.*, Utah Code §§ 13-37-101 - 13-37-203; Cal. Civil Code §§ 1798.83—.84.
30. *See, e.g.*, California Consumer Privacy Act, California A.B. 375 (June 28, 2018), *to be codified at* Cal. Civ. Code §§ 1789.100 – 1798.198 (eff. Jan. 1, 2020) [hereinafter CCPA]; An Act Relating to Internet Privacy, Nevada S.B. 220, 80th Sess. (May 29, 2019), to be codified at Nev. Rev. Stat. 603A (eff. Oct. 1, 2019); Tex. Health & Safety Code §§ 181.001-.207 [hereinafter TMRPA].
31. TMRPA, *supra* note 30.
32. *See, e.g.*, Office of the Texas Attorney General, Texas Medical Records Privacy Act Annual Report (2016) (summarizing the Texas Attorney General's substantial enforcement activities relating to the Texas Medical Records Privacy Act).
33. *See generally* M.A. Rothstein and S.A. Tovino, "California Takes the Lead on Data Privacy Law," *Hastings Center Report* 49, no. 5 (2019), *available at* <https://onlinelibrary.wiley.com/doi/epdf/10.1002/hast.1042> (last visited January 23, 2020).
34. Cal. S.B. 1121, § 9 (Sept. 23, 2018).
35. Cal. A.B. 1355, § 7 (Final Date, 2019).
36. The CCPA defines "deidentified" as "information that cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular consumer, provided that a business that uses deidentified information: (1) Has implemented technical safeguards that prohibit reidentification of the consumer to whom the information may pertain; (2) Has implemented business processes that specifically prohibit reidentification of the information; (3) Has implemented business processes to prevent inadvertent release of deidentified information; and (4) Makes no attempt to reidentify the information." CCPA, *supra* note 30, § 3.
37. The CCPA defines "aggregate consumer information" as "information that relates to a group or category of consumers, from which individual consumer identities have been removed, that is not linked or reasonably linkable to any consumer or household, including via a device. The CCPA excludes from the definition of "aggregate consumer information" one or more individual consumer records that have been deidentified. *Id.*
38. *See, e.g.*, Class Action Complaint and Demand for a Jury Trial, *Dinerstein v. Google*, No. 1-19-cv-04311 (N.D. Ill., June 26, 2019) (illustrating how defendant Google could identify University of Chicago Medical Center patients using health records containing date and time stamps but no other identifiers).
39. *Id.* § 11-12.

The Journal of Law, Medicine & Ethics, 48 S1 (2020): 87-93. © 2020 The Author(s)