Assessing the Thin Regulation of Consumer-Facing Health Technologies

Nicolas P. Terry

I. Introduction

This article addresses the data protection and product safety regulatory models currently applied to consumer-facing health technologies. These are technologies that increasingly support citizen science or other research not currently regulated by the NIH/Common Rule/IRB triad. They also may facilitate corporate "research," the generation or aggregation of health or wellness data that data-driven companies seek to leverage to drive advertising or broader data-broker businesses. Regulatory questions arise because these technologies impact a broad array of ethical, legal, and social issues, in particular challenging our notions of safety, quality, efficacy, and data protection.

The article explains how the design and structures of existing data protection and safety regulation in the U.S. have resulted in exceptionally thin protection for the users of consumer-facing devices and products that rely on or that facilitate consumer collection or aggregation of health and wellness data. It also examines some appealing legislative alternatives to the current thin model used in the U.S. and suggests a framework for prioritizing ameliorative regulation.

II. Scoping

The variety of technologies, platforms, apps, and Direct-to-Consumer (DTC) business models and the emerging use of these for unregulated or underregulated research pose an initial scoping question. It is insufficient to merely point to unregulated conduct or an unregulated space. What, therefore, are the narrowing criteria? Are all technologies included or only "devices"? Do the issues arise within the traditional healthcare system or only outside it in "disruption" space?

The answer seems to be twofold. First, the technologies of concern are consumer-facing. Second, they rotate in some way around consumer-generated or -aggregated data. As to the first, the technologies include not only mobile platforms and their native apps but also web apps, social media platforms, and their apps. Because of the likely technological mediation and data models, the products of interest extend to DTC diagnostic or genetic data devices.

Because data are non-rival, they can exist in more than one place. For example, clinical data held by a health care professional generally would not be viewed as consumer data. However, that same data, once accessed by the data subject through an app or device, would be included as patient-curated. Similarly, health, wellness, or research data generated by a patient's mobile platform or by a wearable device would be included.

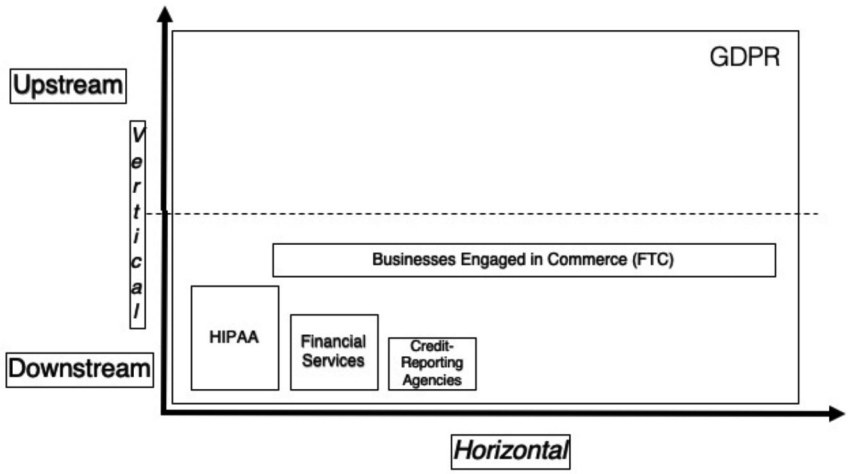
III. Analytical Model

This brief article limits its analyses to the two regulatory systems of greatest importance regarding current consumer-facing health technologies: data protection and safety.[1] To better understand existing regulatory models, their deficiencies, and how they should be reformed, it is helpful to explain these regulatory systems across two axes. The vertical axis describes the quantity or depth of regulation, such as, for example, the strictness of the rules imposed by the regulatory model. The horizontal axis describes the reach of the regulation, the behaviors, products, or industries to which the regulation applies.

Nicolas P. Terry, LL.M., *is the Hall Render Professor of Law and the Executive Director of the Hall Center for Law and Health at Indiana University Robert H. McKinney School of Law.*

The Journal of Law, Medicine & Ethics, 48 S1 (2020): 94-102. © 2020 The Author(s)
DOI: 10.1177/1073110520917034

Figure 1



First, take data protection (*Figure 1*). Rather than all industries being covered by a single data protection regime (as is the case with the European General Data Protection Regulation, or GDPR[2]), in the U.S., different sectors have their own rules. For example, the Gramm–Leach–Bliley Act (GLBA) governs consumer privacy in the financial sector[3] while the HIPAA Privacy, Breach Notification, and Security rules govern patient privacy in most traditional health care settings. However, these rules apply only to HIPAA-covered entities or their "business associates."[4] In contrast, the HIPAA rules seldom will apply to consumer-facing health technologies enabling patient-generated or-curated data as they will be provided by mobile platform manufacturers or sourced from online app stores.

Absent specific sectoral data protection, industries such as those that supply consumer-facing web or device apps, are not subject to any robust form of federal data protection. While the Federal Trade Commission (FTC) has overarching jurisdiction, even overlapping with HIPAA in some health care cases,[5] its prohibitions on "unfair or deceptive acts or practices in or affecting commerce"[6] are thin and limit agency actions to parsing privacy policies or other representations by sellers[7] or, occasionally, pushing back against repeat offenders.[8]

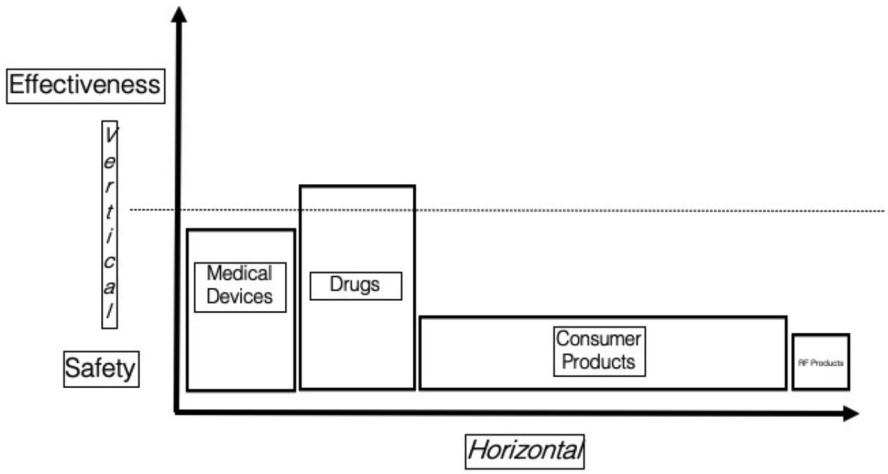
Even where the HIPAA rules do apply, they are somewhat limited on the vertical axis. Those rules only regulate downstream, post-collection interactions with patient data such as unauthorized disclosure (The Privacy Rule), not upstream, collection-limiting interactions such as the data minimization or purpose limitations required by the GDPR[9] or the somewhat exceptional U.S. prohibitions on the collection of genetic data provided for in the Genetic Information Nondiscrimination Act of 2008.[10]

The variety of technologies, platforms, apps, and Direct-to-Consumer (DTC) business models and the emerging use of these for unregulated or underregulated research pose an initial scoping question. It is insufficient to merely point to unregulated conduct or an unregulated space. What, therefore, are the narrowing criteria? Are all technologies included or only "devices"? Do the issues arise within the traditional healthcare system or only outside it in "disruption" space?

Similar limitations play out regarding the safety of consumer-facing web or device apps (*Figure 2*). Most health-related drugs and devices will be regulated by the FDA. However, the overwhelming majority of consumer-facing products will be regulated separately by the U.S. Consumer Product Safety Commission (CPSC)[11] while some FDA or non-FDA devices may be subject to other (and narrow, domain-specific) regu-

The Journal of Law, Medicine & Ethics, 48 S1 (2020): 94-102. © 2020 The Author(s)

Figure 2



latory requirements such as the Federal Communications Commission's rules on devices emitting radio frequencies.[12] On the vertical axis of product safety, and stated in broad terms, FDA drug regulation is arguably the strongest (and stronger than its regulation of devices or food). The CPSC has a relatively shallow safety jurisdiction; although it does exercise regulatory powers to ban some products or their components,[13] most of its jurisdiction is reactive, banning or recalling products proven to be dangerous.[14] In this regard, the CPSC's role in product safety somewhat resembles the FTC's role in the data protection space.

Overall, although somewhat fragmented, the regulation of products is less susceptible to regulatory arbitrage[15] than current U.S. data protection laws. This is because the regulatory touchstone is a product type (for example, a device or a drug) rather than a type of data custodian (for example, a HIPAA-covered entity).

The regulatory touchstone for the regulation of health-related product safety is a subset of product: "device" as defined in the Federal Food, Drug, and Cosmetic Act.[16] On the horizontal axis, albeit already one limited to the medical domain, "device" has had an expansive meaning within that domain. It applies to software (software as medical device or SaMD) as well as hardware[17] and is not limited by market, applying equally to products distributed directly to consumers and through health care providers.[18]

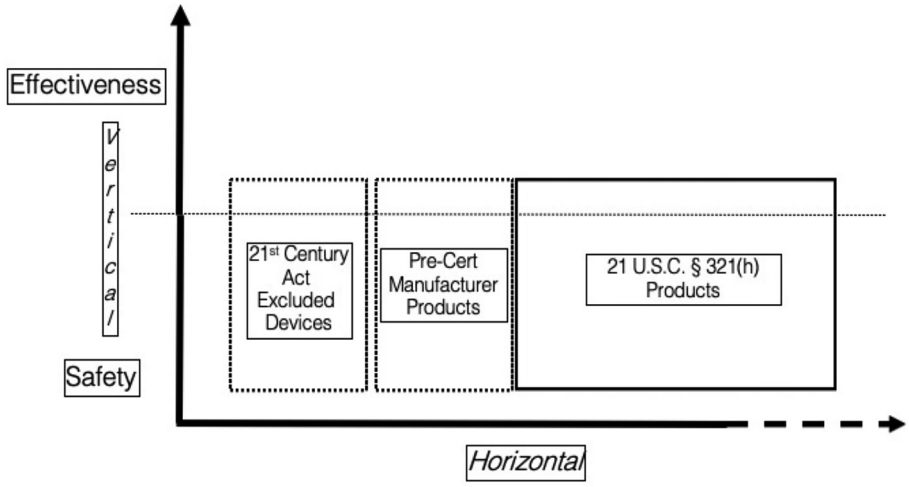
Recently, however, that conception of medical device has begun to shrink. This may be a function of the FDA and Congress believing that large swathes of consumer-facing devices are very low risk or that overregulation was stifling innovation.[19] Whatever the reason, the FDA first started to shrink the products it would regulate by issuing sub-regulatory guidances noting that it would exercise regulatory discretion with regard to certain types of products.[20] In 2016 Congress went further in the 21st Century Cures Act (Cures), excluding "a software function that is intended ... for maintaining or encouraging a healthy lifestyle and is unrelated to the diagnosis, cure, mitigation, prevention, or treatment of a disease or condition"[21] (*Figure 3*).

The FDA's Digital Health Innovation Action Plan[22] likely will result in still more consumer-facing devices being removed from direct regulatory scrutiny. The Action Plan's centerpiece is the agency's Precertification (Pre-Cert) Program that certifies manufacturers and their safety-testing protocols that evidence "excellence."[23] The internal processes of these certified manufacturers are then used as a surrogate for traditional agency review.[24] Manufacturers who have been certified in the Pre-Cert pilot program include several manufacturers of consumer-facing platforms and apps such as Apple, Fitbit, and Samsung. The devices that are no longer subject to traditional FDA processes either, as is the case with Pre-cert products, will attract reduced regulation (for example, post-marketing surveillance only) or with "devices" exempted by the Cures Act, henceforth will be subject to the reduced protection offered by the CPSC or ex-post state products liability law.[25]

Device regulation is also limited on the vertical axis. Historically, the FDA has approved devices that are reasonably safe and "effective for a particular use"[26] or efficacy. These are relatively limited criteria given that, increasingly, consumer-facing health and wellness devices are viewed as substitutes for aspects of clinical care, such as preventative care, physical surveillance, and chronic disease management. Contemplation of

The Journal of Law, Medicine & Ethics, 48 S1 (2020): 94-102. © 2020 The Author(s)

Figure 3



such substitutions suggests that consumers would benefit from information not only about a device's safety and efficacy but also its comparative effectiveness or cost effectiveness with regard to other devices or treatments.[27] The FDA also is noticeably reticent about reviewing devices for data protection risks. The FDA has partially recognized these and has issued sub-regulatory guidances to device manufacturers about security risks,[28] and advanced device cybersecurity is one of the pillars of the agency's *Medical Device Safety Action Plan*.[29]

There have been a small number of attempts to patch, or at least better explain or clarify, the fragmented nature of both regulations and regulators. Sub-regulatory guidances issued by the FDA are examples. Further, in 2016 the Office of the National Coordinator, the FTC, and the FDA jointly issued an interactive tool to advise health app developers to the potential applicability of HIPAA, the FDA's device regulation, the FTC's jurisdiction over deceptive or unfair acts, and the FTC's Breach Notification Rule for personal health records.[30]

Overall, however, the data protection and safety regulatory models applicable to health or health research consumer-facing technologies exhibit critical levels of underregulation and considerable fragmentation at both the regulation and regulator levels. Their underregulation is most obvious on the vertical axis, with U.S. models applying quite low levels of protection for consumers, particularly given the sensitive nature of health and wellness information and the potential for surveillance and discriminatory misuse.

Fragmentation is most obvious on the horizontal axis, engendering consumer confusion as to what regulation or which regulator applies to a technology or, worse, encouraging businesses to exploit differential regulatory models through arbitrage. The most obvious example of the latter is the ability of data brokers to essentially recreate clinical records (that, in identified form, are protected by HIPAA) outside HIPAA-regulated space with social media and other types of medically inflected data.[31]

A broader question about regulatory fragmentation also is emerging: are questions about data protection and safety sufficiently separate (witness the concerns over the security of medical devices[32]) to justify discrete regulatory systems or — and this seems to be even more crucial at the data-product intersection — would a more holistic model be preferable? This is a question that appears particularly critical as data and device merge such as in products that make extensive use of artificial intelligence.[33]

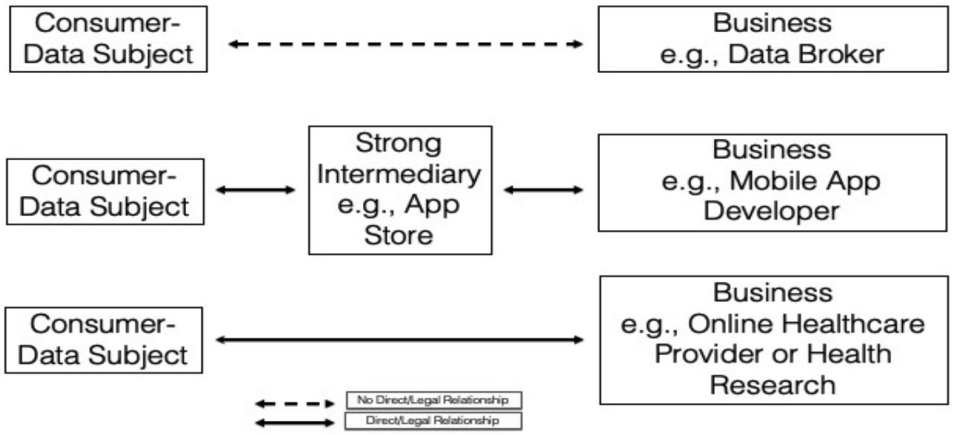
IV. Legislative Models

The obvious but politically unlikely model for reforming the regulatory models applicable to consumer-facing technologies is twofold. First, the regulatory frameworks should be far more inclusive as to the producers or products they pertain to (the horizontal axis). Second, they should be more robust in their substantive regulation (the vertical axis).

The GDPR data protection framework is most typically favored by pro-privacy reformers seeking to improve the data protection applicable to consumer-facing health technologies in the U.S. In broad terms, the GDPR increases data protection and minimizes regulatory arbitrage by using broad inclusive language such as "personal data," "data subject," and "processing" to define the regulation's horizontal scope.[34] On the vertical axis, it sets out clear principles by which to

The Journal of Law, Medicine & Ethics, 48 S1 (2020): 94-102. © 2020 The Author(s)

Figure 4



limit data collection and processing, such as transparency, a purpose limitation, and data minimization.[35]

In the United States, the closest analogue to the GDPR is California's Consumer Privacy Act of 2018, effective in January 2020.[36] That statute promotes (initially at least) broad applicability on the horizontal axis by establishing "consumer" rights and "business" duties (rather than protecting only narrow domains) and expressly including biometric and health insurance information.[37] On the vertical axis, the statute primarily relies on a transparency model requiring data custodians to disclose what information they hold about a data subject and whether it is being sold or otherwise disclosed. The data subject can stop the sale of the information and cannot be discriminated against in service or if they exercise their rights.[38] However, domain carveouts for HIPAA entities and human subjects research data[39] derogate somewhat from what at first sight seemed domain agnosticism. As a result, the statute perpetuates some data protection fragmentation on the horizontal axis. Notwithstanding, even with that flaw, the statute dramatically increases the protection of data collected or generated by consumer-facing health technologies as evidenced by the attempts of Google and other consumer-facing technology companies to weaken the legislation before it can take effect.[40] Not surprisingly, the California statute has been viewed as a possible model for enactment by other states.[41] The California statute also seems to have engendered corporate support for increased federal data protection.[42] However, once scrutinized, those interests actually favor a series of lesser protections that, crucially, would be accompanied by a provision preempting the California statute and any state laws that may mimic it.[43]

There *is* legislative interest in extending data protection. It finds expression either in general statutes such as California's or enactments that protect, for example, narrower slices of data such as biometric data.[44] However, the same cannot be said of device safety. Indeed, all indications are that the FDA remains committed to its existing model and its Pre-cert carve-out, notwithstanding questions that have been raised as to both its functioning and its statutory basis.[45] For example, the FDA has not only released an upgraded framework for Pre-cert but also indicated that it may adopt a similar structure for other challenging SaMD products such as "unlocked" AI/ML algorithms.[46]

V. Policy Frameworks

In the absence of broad protections that feature domain agnostic applicability (horizontal axis) and robust, multi-factor protections (vertical axis), policymakers need to concentrate on more specific problems and solutions. One way to prioritize and calibrate regulatory and non-regulatory interventions is through examining the extent to which market or similar relationships can achieve at least basic protections.

Thus, regulatory priority should be given to situations where there is no direct or market relationship between the consumer and the data custodian such that questions of consent to collection or processing could be negotiated (*Figure 4*). This is most clearly exemplified by the data-broker industry that is collecting both deidentified clinical data and identified or identifiable consumer-generated health or research data.[47] Other than the specific authority enjoyed by the FTC under the Fair Credit Reporting Act to regulate some data brokers who are also consumer reporting agencies,[48] the only meaningful data-broker legislation is Vermont's: a 2018 statute requires data brokers

The Journal of Law, Medicine & Ethics, 48 S1 (2020): 94-102. © 2020 The Author(s)

to register with the state (over 120 have so far[49]) and to note whether they permit consumers to opt-out of data collection.[50]

Consumers have no relationship with such data custodians and, in all likelihood and unless they live in Vermont, do not know their identity, whether they have data relating to them, or how they can be contacted. Notwithstanding the many earnest government reports noting the problems associated with an unrestrained data broker industry, there has been no meaningful federal response.[51]

At the other extreme, of course, there will be situations where there is a direct (and likely market) relationship between the consumer and the data custodian or device/service distributor. In such cases, a rational expectation would be that, for example, consumers will be attracted to platforms that espouse greater privacy and security or at least make rational tradeoffs between data protection and other features. This is certainly the bet that Apple is making to differentiate their products and services from other technology companies interested in the health space such as Facebook and Google.[52] For example, Apple has introduced an email relay that lets users receive email from third parties while keeping their actual email addresses private.[53] Similarly, Apple Pay and Apple Card enable privacy and security seldom seen in the financial services space.[54]

The consumer-facing health app space provides an opportunity for developers to differentiate themselves on the basis of data protection. However, few do. Fertility or menstrual cycle tracking apps are a good example with the leading apps selling deidentified, aggregated data not only to researchers and marketing companies but also employers and health insurers.[55] In contrast, "Euki," an app developed by the Women Help Women non-profit organization keeps all the data the user generates on-device not in the cloud such that only the user and neither the platform owner nor the developer has access.[56]

Of course, some consumers (perhaps undereducated as to the seriousness of the tradeoff) may place a high value on "free" services that are provided in exchange for personal information. At the extreme, this conjures up the dystopian idea of "surveillance capitalism" whereby businesses provide free access to social interactions, search, or even healthcare in exchange for untold amounts of consumer, including health, data.[57] The dominant data protection model in the direct relationship scenarios remains bankrupt notice and consent, which provides at best illusory "protection."[58] Although some more privacy-protective companies have begun to use opt-in[59] rather than the usual opt-out version, overall, even where there is some direct relationship, some additional data regulation will still be required to correct market failure. The regulatory priority in such cases should be to consign notice and comment to history and impose a California-like "right to request that a business delete any personal information about the consumer which the business has collected from the consumer."[60] Additionally, some data minimization based on a purpose limitation should be considered.

Regulatory priority should be given to situations where there is no direct or market relationship between the consumer and the data custodian such that questions of consent to collection or processing could be negotiated. This is most clearly exemplified by the data-broker industry that is collecting both deidentified clinical data and identified or identifiable consumer-generated health or research data.

In between these two extremes (market/no market relationship) are situations where the relationship between consumer data subject and business data custodian is mediated in some way by a powerful or responsible infomediary or intermediary, enabling private ordering or soft law. As to the former a recent example is Google's decision to stop taking ads for "unproven or experimental medical techniques," specifically targeting ads for stem cell therapy.[61]

Platform owners are also market-aligned regulators, particularly powerful intermediaries capable of imposing technical barriers to curtail abusive behaviors of businesses using their platforms. For example, both Google and Apple have introduced software on their platforms to intercept robocalls made to consumers.[62]

Additionally, some market-dominating platforms require that all apps must be distributed from app stores controlled by the platform owners. Thus, Apple's

The Journal of Law, Medicine & Ethics, 48 S1 (2020): 94-102. © 2020 The Author(s)

App Store rules prohibit developers from using "data gathered in the health, fitness, and medical research context ... for advertising or other use- based data mining purposes other than improving health management." The Apple App Store also requires that developers of apps that use the HealthKit framework publish privacy policies and imposes additional restrictions on developers whose apps use HealthKit to support clinical research.[63] The credibility of such intermediaries in protecting consumers data and safety can be increased when the businesses have strong internal ethics boards or similar machinery, although the opposite is also true and credibility is lessened when such boards fail.[64]

In the healthcare space, IRBs have long been the quintessential intermediaries, protecting research subjects from overreaching by researchers and some consumer-facing technologies leverage IRBs by requiring their participation in technologically-mediated research.[65] However, the majority of the citizen research considered herein will take place without IRB approval or the participation of other professional intermediaries by approaching consumers directly, as in the case of DTC genetic testing.

Traditionally physicians have played an important role in mitigating the risks suffered by patients. Not only do they owe duties of confidentiality regardless of the HIPAA rules and are required intermediaries in the distribution of prescription devices, but they are also important infomediaries with regard to over-the-counter drugs, devices, and increasingly apps. As such, there are some opportunities for healthcare providers to reassert their role by curating or recommending certain consumer-facing technologies that intrinsically or legally do not cast providers as learned intermediaries. However, the incentives are not well aligned here because healthcare professionals or institutions could face some legal jeopardy if they recommend or curate consumer-facing technologies that implicate consumer privacy or safety.[66]

VI. Conclusion

The rate of iteration among companies developing consumer-facing healthcare technologies generating massive amounts of data continues to be rapid. For example, Apple recently announced the use of its platform and wearable technologies in novel hearing, women's health, and heart and movement studies in partnership with major research institutions such as NIH's National Institute of Environmental Health Sciences, Brigham and Women's Hospital, and the University of Michigan.[67] Equally, DTC genetic testing has exploded with more than 12 million persons participating and driving an increasingly popular personal genealogy industry.[68]

However, regulation has not kept up. Worse, under-regulation attracts businesses with dubious ethics while the regulatory uncertainty tends to keep responsible businesses on the sidelines. Notwithstanding the absence of the political will to advance major legislation, there are plenty of opportunities for patchwork fixes, and these can be prioritized by understanding both the regulatory models as defined on both their vertical and horizontal axes and the relationship (or lack thereof) between consumers and businesses, together with the hope that new intermediaries and infomediaries will emerge to improve the data protection and safety environments.

Acknowledgment

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

My thanks to Anthony Singer, J.D./M.P.H. candidate for his editorial assistance.

Note

The author has no conflicts of interest to disclose.

References

1. *See generally* N.P. Terry and T. D. Gunter, "Regulating Mobile Mental Health Apps," *Behavioral Sciences & the Law* 36 (2018):136-144; K. Huckvale, J. Torous, and M.E. Larsen, "Assessment of the Data Sharing and Privacy Practices of Smartphone Apps for Depression and Smoking Cessation" *JAMA Network Open* 2, no. 4 (2019).
2. Commission Regulation 2016/679 of Apr 27, 2016, On the Protection of Natural Persons with regard to the Processing of Personal Data and on the Free Movement of such Data, and Repealing Directive 95/46/EC, 2016 O.J. (L 119) 1.
3. Gramm-Leach-Bliley Act, Pub. L. No. 106-102, § 501, 113 Stat. 1338, 1436–37.
4. 45 C.F.R. § 160.102(b).
5. LabMD, Inc., "In the Matter of," *available at* <https://www.ftc.gov/enforcement/cases-proceedings/102-3099/labmd-inc-matter>_(last visited January 29, 2020) (the overlap with HIPAA was not at issue in LabMD, Inc. v. Federal Trade Commission, 894 F.3d 1221 (11th Cir. 2018)).
6. Section 5(a) Federal Trade Commission Act, 15 USC § 45.
7. *See, e.g.*, C. Tressler, "FTC Presses Aura Over Blood Pressure App," *available at* <https://www.consumer.ftc.gov/blog/2016/12/ftc-presses-aura-over-blood-pressure-app>_(last visited January 29, 2020).
8. *See, e.g.*, Federal Trade Commission, "Wyndham Settles FTC Charges It Unfairly Placed Consumers' Payment Card Information at Risk," *available at* <https://www.ftc.gov/news-events/press-releases/2015/12/wyndham-settles-ftc-charges-it-unfairly-placed-consumers-payment> (last visited January 29, 2020).
9. *See generally* N. Terry, "Regulatory Disruption and Arbitrage in Healthcare Data Protection," *Yale Journal of Health Policy, Law & Ethics* 17, no. 1 (2017): 143-208, 152-54.
10. Pub. L. No. 110-233, 122 Stat. 881 (2008).

The Journal of Law, Medicine & Ethics, 48 S1 (2020): 94-102. © 2020 The Author(s)

https://doi.org/10.1177/1073110520917034 Published online by Cambridge University Press

11. "United States Consumer Product Safety Commission," *available at* <https://www.cpsc.gov> (last visited January 31, 2020).
12. Federal Communications Commission, "Equipment Authorization," *available at* <https://www.fcc.gov/engineering-technology/laboratory-division/general/equipment-authorization> (last visited January 31, 2020); *see, e.g.*, 47 CFR § 2.907. Other regulatory agencies on the horizontal axis include the National Highway Traffic Safety Administration (motor vehicles) and the United States Environmental Protection Agency (some poisons, such as pesticides).
13. *E.g.*, lead-containing paint, 16 C.F.R. Part 1303.
14. *E.g.*, some type of trampoline, United States Consumer Product Safety Commission, "Super Jumper Recalls Trampolines Due to Fall and Injury Hazards," *available at* <https://www.cpsc.gov/Recalls/2019/Super-Jumper-Recalls-Trampolines-Due-to-Fall-and-Injury-Hazards> (last visited January 31, 2020).
15. *See generally* Terry, *supra* note 9.
16. 21 U.S.C. § 321(h).
17. *See generally* Food & Drug Administration, U.S. Department of Health and Human Services, "Software as a Medical Device (SaMD)," *available at* <https://www.fda.gov/medical-devices/digital-health/software-medical-device-samd> (last visited January 31, 2020).
18. *See, e.g.*, Food & Drug Administration, U.S. Department of Health and Human Services, "Direct-to-Consumer Tests," *available at* <https://www.fda.gov/medical-devices/vitro-diagnostics/direct-consumer-tests> (last visited January 31, 2020).
19. *See generally* Food & Drug Administration, U.S. Department of Health and Human Services, "FDA In Brief: FDA Takes New Steps to Advance Risk-based Regulation of Digital Health Tools," *available at* <https://www.fda.gov/news-events/fda-brief/fda-brief-fda-takes-new-steps-advance-risk-based-regulation-digital-health-tools> (last visited January 31, 2020).
20. *See, e.g.*, Food & Drug Administration, U.S. Department of Health and Human Services, "Clinical and Patient Decision Support Software: Draft Guidance for Industry and Food and Drug Administration Staff," *available at* <https://www.fda.gov/media/109618/download> (last visited January 31, 2020).
21. 21 U.S.C. § 360j(o)(1)(B).
22. Food & Drug Administration, U.S. Department of Health and Human Services, "Digital Health Innovation Action Plan," *available at* <https://www.fda.gov/downloads/MedicalDevices/DigitalHealth/UCM568735.pdf> (last visited January 31, 2020).
23. Food & Drug Administration, U.S. Department of Health and Human Services, "Digital Health Software Precertification (Pre-Cert) Program," *available at* <https://www.fda.gov/MedicalDevices/DigitalHealth/DigitalHealthPreCertProgram/default.htm> (last visited January 31, 2020).
24. *Id.*
25. *See generally* N. Terry and L.F. Wiley, "Liability for Mobile Health and Wearable Technologies," *Annals of Health Law* 25, no. 2 (2016): 62-97, 86-89 (2016); *see also* J. Steinberg, "Fitbit Sleep-Tracker Settlement Slated for September Hearing," *available at* <https://news.bloombergenvironment.com/product-liability-and-toxics-law/fitbit-sleep-tracker-settlement-slated-for-september-hearing> (last visited January 31, 2020).
26. Food & Drug Administration, U.S. Department of Health and Human Services, "FDA's Role in Regulating Medical Devices," *available at* <https://www.fda.gov/medical-devices/home-use-devices/fdas-role-regulating-medical-devices> (last visited January 31, 2020).
27. *See generally* M. Drummond, R. Tarricone, and A. Torbica, "Economic Evaluation of Medical Devices," *available at* <https://oxfordre.com/economics/view/10.1093/acrefore/9780190625979.001.0001/acrefore-9780190625979-e-105> (last visited January 31, 2020).
28. *See, e.g.*, Food & Drug Administration, U.S. Department of Health and Human Services, "Content of Premarket Submissions for Management of Cybersecurity in Medical Devices: Draft Guidance for Industry and Food and Drug Administration Staff," *available at* <https://www.fda.gov/media/119933/download> (last visited January 31, 2020); *see generally* Food & Drug Administration, U.S. Department of Health and Human Services, *Cybersecurity*, *available at* <https://www.fda.gov/medical-devices/digital-health/cybersecurity> (last visited January 31, 2020).
29. Food & Drug Administration, U.S. Department of Health and Human Services, "Medical Device Safety Action Plan: Protecting Patients, Promoting Public Health," *available at* <https://www.fda.gov/about-fda/cdrh-reports/medical-device-safety-action-plan-protecting-patients-promoting-public-health> (last visited January 31, 2020).
30. Federal Trade Commission, "Mobile Health Apps Interactive Tool," *available at* https://www.ftc.gov/tips-advice/business-center/guidance/mobile-health-apps-interactive-tool> (last visited January 31, 2020).
31. *See generally* N. Terry, "Big Data Proxies and Health Privacy Exceptionalism," *Health Matrix* 24, no. 1 (2014): 65-108.
32. *See, e.g.*, Van Wagenen, "Medical Device Vulnerabilities Continue to Plague the Industry," *available at* <https://healthtechmagazine.net/article/2018/12/medical-device-vulnerabilities-continue-plague-industry> (last visited January 31, 2020).
33. *See generally* N. Terry, "Of Regulating Healthcare AI and Robots," *Yale Journal of Law and Technology* 21, no. 3 (2019), *available at* <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3321379> (last visited January 31, 2020).
34. Commission Regulation 2016/679 of Apr 27, 2016, On the Protection of Natural Persons with regard to the Processing of Personal Data and on the Free Movement of such Data, and Repealing Directive 95/46/EC, 2016 O.J. (L 119) 33.
35. Commission Regulation 2016/679 of Apr 27, 2016, On the Protection of Natural Persons with regard to the Processing of Personal Data and on the Free Movement of such Data, and Repealing Directive 95/46/EC, 2016 O.J. (L 119) 35.
36. Cal. Civ. Code §§ 1798.100 to 1798.198.
37. Cal. Civ. Code §§ 1798.140(b), 1798.140(k).
38. Cal. Civ. Code §§ 1798.105-125.
39. Cal. Civ. Code § 1798.145(c).
40. *See, e.g.*, N. Lindsey, "Google, Other Tech Companies Trying to Dilute CCPA with AdTech Exemption," *available at* <https://www.cpomagazine.com/data-protection/google-other-tech-companies-trying-to-dilute-ccpa-with-adtech-exemption/> (last visited January 31, 2020).
41. K. Murphy, "California Privacy Law Sets National Agenda as Federal Talks Fizzle," *available at* <https://www.politico.com/states/california/story/2019/08/08/california-privacy-law-sets-national-agenda-as-federal-talks-fizzle-1126208> (last visited January 31, 2020).
42. I. Lapowsky, "Get Ready for a Privacy Law Showdown in 2019," *available at* <https://www.wired.com/story/privacy-law-showdown-congress-2019/> (last visited January 31, 2020).
43. Committee on Commerce, Science & Transportation, U.S. Senate, "Hearings: Examining Safeguards for Consumer Data Privacy," *available at* <https://www.commerce.senate.gov/public/index.cfm/2018/9/examining-safeguards-for-consumer-data-privacy> (last visited January 31, 2020).
44. *See, e.g.*, 740 ILCS 14/1; Tex. Bus. & Com. Code § 503.001; RCW 19.375 et seq.
45. Letter from Elizabeth Warren, U.S. Senator from Massachusetts; Patty Murray, U.S. Senator from Washington; and Tina Smith, U.S. Senator from Minnesota; to Scott Gottlieb, Commissioner, U.S. Food and Drug Administration, and Jeffrey Shuren, Director, Center for Devices and Radiological Health, U.S. Food and Drug Administration, *available at* <https://www.warren.senate.gov/imo/media/doc/2018.10.10%20Letter%20to%20FDA%20on%20regulation%20of%20software%20as%20medical%20device.pdf> (last visited January 31, 2020).

The Journal of Law, Medicine & Ethics, 48 S1 (2020): 94-102. © 2020 The Author(s)

46. Food & Drug Administration, U.S. Department of Health and Human Services, "Proposed Regulatory Framework for Modifications to Artificial Intelligence/Machine Learning (AI/ML)-Based Software as a Medical Device (SaMD) - Discussion Paper and Request for Feedback, 3," *available at* <https://www.fda.gov/media/122535/download> (last visited January 31, 2020).
47. S. Melendez and A. Pasternack, "Here Are the Data Brokers Quietly Buying and Selling Your Personal Information," *available at* <https://www.fastcompany.com/90310803/here-are-the-data-brokers-quietly-buying-and-selling-your-personal-information> (last visited January 31, 2020).
48. 15 U.S.C. §§ 1681–1681x.
49. S. Melendez, "A Landmark Vermont Law Nudges Over 120 Data Brokers Out of the Shadows," *available at* <https://www.fastcompany.com/90302036/over-120-data-brokers-inch-out-of-the-shadows-under-landmark-vermont-law> (last visited January 31, 2020).
50. H.B.764, 2017-2018 Gen. Assemb. 74th Biennial Sess. (Vt. 2018).
51. N. Terry, "Navigating the Incoherence of Big Data Reform Proposals," *Journal of Law, Medicine, & Ethics* 43, no. 1 (2015): 44-47, 44.
52. Apple, "Privacy," *available at* <https://www.apple.com/privacy/> (last visited January 31, 2020).
53. Apple, "Sign in with Apple," *available at* <https://developer.apple.com/sign-in-with-apple/> (last visited January 31, 2020).
54. Apple, "Apple Card: Privacy and Security," *available at* <https://www.apple.com/apple-card/privacy-security/> (last visited January 31, 2020).
55. D. Harwell, "Is Your Pregnancy App Sharing Your Intimate Data with Your Boss?" *available at* <https://www.washingtonpost.com/technology/2019/04/10/tracking-your-pregnancy-an-app-may-be-more-public-than-you-think/?> (last visited January 31, 2020).
56. WomenHelpWomen, "Euki App," *available at* <https://abortionpillinfo.org/en/page/378/euki-app> (last visited January 31, 2020).
57. *See generally* S. Zuboff, "Big Other: Surveillance Capitalism and the Prospects of an Information Civilization," *Journal of Information Technology* 30, no. 1 (2015): 75-89.
58. *See generally* R.H. Sloan and R. Warner, "Beyond Notice and Choice: Privacy, Norms, and Consent," *Journal of High Technology Law* 14, no. 2 (2014): 370-407, at 390.
59. Apple, "Improving Siri's Privacy Protections," *available at* <https://www.apple.com/newsroom/2019/08/improving-siris-privacy-protections/> (last visited January 31, 2020).
60. Cal. Civ. Code § 1798.105 (a).
61. Google, "Advertising Policies: Healthcare and medicines," *available at* <https://support.google.com/adspolicy/answer/176031> (last visited January 31, 2020).
62. M. Purdue, "Apple Introduces New Call Blocking Software with iOS 13 to Combat Robocalls," *available at* <https://www.usatoday.com/story/tech/2019/06/06/apple-combats-robocalls-call-block-features-ios-13-software/1361696001/ (last visited October 4, 2019).
63. Apple, *Protecting User Privacy*, *available at* <https://developer.apple.com/documentation/healthkit/protecting_user_privacy> (last visited January 31, 2020).
64. K. Piper, *Exclusive: Google Cancels AI Ethics Board in Response to Outcry*, *available at* <https://www.vox.com/future-perfect/2019/4/4/18295933/google-cancels-ai-ethics-board> (last visited January 31, 2020).
65. J. Comstock, *Apple Adds Mandatory IRB Ethics Review to Researchkit Guidelines*, *available at* <https://www.mobihealthnews.com/43045/apple-adds-mandatory-irb-ethics-review-to-researchkit-guidelines> (last visited January 31, 2020).
66. Terry and Wiley, *supra* note 25.
67. Apple, *Apple Announces Three Groundbreaking Health Studies*, *available at* <https://www.apple.com/newsroom/2019/09/apple-announces-three-groundbreaking-health-studies/> (last visited January 31, 2020).
68. S. Bowen and M.J. Khoury, *Consumer Genetic Testing Is Booming: But What are the Benefits and Harms to Individuals and Populations?*, *available at* <https://blogs.cdc.gov/genomics/2018/06/12/consumer-genetic-testing/> (last visited January 31, 2020).

The Journal of Law, Medicine & Ethics, 48 S1 (2020): 94-102. © 2020 The Author(s)