General-Purpose Privacy Regulation and Translational Genomics

William McGeveran and Caroline Schmitz

Introduction

At one time, when the study of genetics was newer, only a limited set of comparatively elite institutions worked with genetic and genomic data, in either clinical or research settings. These entities generally concentrated their legal compliance efforts on regulatory schemes established specifically to govern medical information, and sometimes tailored to genetic information in particular.[1] These regimes include the Privacy Rule of the Health Insurance Portability and Accountability Act of 1966, the Common Rule, the Genetic Information Nondiscrimination Act, and state genetic privacy laws.[2]

Genomic data is no longer contained within an insulated bubble of specialized legal regimes operating on a limited set of leading organizations. As discussed below, new types of entities, new legal developments, and new technological understanding mean the rules that have applied inside that bubble — while still vitally important — no longer tell the whole story of genetic privacy law. As research and technology relating to genomic information have developed exponentially, a similar increase has occurred in the awareness of and interest in the potential of genomics,[3] and as a result new parties are now utilizing genetic information in new ways.[4] Translational genomics — broadly, the application of genomic research for clinical purposes beyond pure research[5] — has moved beyond the bounds of its regulatory bubble. This is the natural consequence of several factors.

First, genetics and genomics are no longer the sole province of a limited number of highly regulated entities, such as hospitals, universities, and traditional private research institutions. In the past, this small community shared similar norms and values informed by those of the medical profession and the pursuit of academic inquiry. Today, enterprises motivated more directly by profit play a much greater role in translational genomics. Direct-to-consumer (DTC) companies, such as 23andMe, have entered the market and grown rapidly, both capitalizing on and driving

William McGeveran, J.D., *is Associate Dean for Academic Affairs and Julius E. Davis Professor of Law at the University of Minnesota. He is the author of a casebook and many articles on data privacy law, and serves as reporter for a Uniform Law Commission project to draft a model state privacy law.*
Caroline Schmitz, J.D., *graduated cum laude from the University of Minnesota Law School in May 2019. While in law school, she participated in the Data Compliance Practicum and the Consumer Protection Clinic. She now works for the Federal Trade Commission (FTC) in its Division of Privacy & Identity Protection. Caroline participated in co-authoring this article in her personal capacity, not as a representative of the FTC, and the views expressed are her own and not necessarily those of the Commission or any individual Commissioner.*

The Journal of Law, Medicine & Ethics, 48 (2020): 142-150. © 2020 The Author(s)
DOI: 10.1177/1073110520917002

decreased cost and increased accessibility of genetic testing.[6] By the start of 2019, over twenty-six million people had submitted a DNA sample to a direct-to-consumer genetic testing company.[7]

DTC enterprises are hardly the only new actors engaging with genetic and genomic data. Pharmaceutical companies have expanded their traditional research scope to encompass genetic information. Pharmaceutical giant GlaxoSmithKline recently struck a $300 million deal with 23andMe to use the company's deidentified, aggregate consumer data for drug development research.[8] Additionally, hybridized insurance companies acting outside their HIPAA-covered business lines, such as a noncovered component offering life or disability insurance, bring health care related information outside of the scope of the traditionally applicable laws like HIPAA.[9] Law enforcement agencies are also utilizing genetic information in new ways in their investigation and prosecution of crime, including drawing on databases maintained by DTC companies.[10] In the United States, all these new players frequently fall outside the confines of traditional privacy laws for health or genetic information, but most are covered by more broadly applicable privacy laws.

Genomic data is no longer contained within an insulated bubble of specialized legal regimes operating on a limited set of leading organizations. As discussed below, new types of entities, new legal developments, and new technological understanding mean the rules that have applied inside that bubble — while still vitally important — no longer tell the whole story of genetic privacy law.

Second, privacy regulation in the United States and abroad is shifting and expanding. Historically, privacy law in the United States has been limited and each enactment has imposed requirements only on particular industry sectors.[11] Today, regulators outside health care are beginning to investigate privacy compliance in health-related institutions. Recent legislative proposals in Congress and the states cast somewhat wider nets than the narrow sectoral laws of the past.[12] Meanwhile, in the rest of the world, the broadly applicable framework exemplified by the European Union's General Data Protection Regulation (GDPR) has been imitated widely in countries from Brazil to Israel to Japan since it came into effect in 2018.

Finally, a growing skepticism about deidentification, both broadly and in reference to genomics in particular, could drive legal change in this area. Due to its intrinsically unique nature, genetic data raises particularly acute skepticism about the adequacy of deidentification as a measure to ensure confidentiality.[13] Multiple studies have established how an individual can be reidentified in some cases from a purportedly deidentified data set.[14] Yet a 2018 revision to "modernize, strengthen, and make more effective" the Common Rule[15] expanded the exemptions for secondary research involving deidentified information or biospecimens, while also committing to a review of its scope on a routine basis.[16] For example, information or biospecimens are no longer required to be "existing" at the time of exemption, thus data under this exemption may be both retrospective and prospective.[17] Some public comments in response to the Notice of Proposed Rulemaking argued that all biospecimens are inherently identifiable. Although regulators ultimately did not adopt a position against all reliance on deidentification in the final rule, the trend toward stricter standards is clear, and the new rule contemplates continuous reexamination of the question.[18]

In light of these trends and developments, a responsible overview of privacy law applicable to translational genomics cannot be limited to the "usual suspects," such as HIPAA or the Common Rule, and must also consider how general-purpose privacy laws affect genetic information. Part I of this article provides a background of general privacy law beyond the health sector. Part II focuses on the ways those general privacy laws affect the health sector and genomic information in particular and considers potential consequences of this broader understanding of privacy law as it applies to translational genomics.

I. Privacy Law Beyond the Health Sector

Most U.S. privacy law has two features that distinguish it from privacy law in other countries: U.S. law is sectoral and it is based on a "consumer protection" model. By contrast, in most other jurisdictions, personal information is safeguarded by omnibus laws rooted in a "data protection" model. The likely reasons for these differences include cultural influences and divergent constitutional treatment of rights to both privacy and free expression. Whatever its origins, the broad difference is widely understood.[19]

The Journal of Law, Medicine & Ethics, 48 (2020): 142-150. © 2020 The Author(s)

Much of U.S. privacy law is narrow, with particular statutes regulating a single industry, type of technology, or population. So, for example, the Gramm-Leach Bliley Act governs handling of personal data in the financial sector, the Video Privacy Protection Act protects privacy for customers at video rental or streaming services, and the Children's Online Privacy Protection Act regulates children's online personal information. In other words, most U.S. statutes are tailored to address a particular harm within a particular context. To date, most traditional entities operating within areas like health care or biomedical research were also regulated in ways unique to that sector. HIPAA, the Common Rule, and GINA are classic examples of such sectoral statutes. HIPAA applies only to patients' personal health information when handled by specific "covered entities" — such as physicians, hospitals, or insurance companies — and their "business associates." The Common Rule regulates only the treatment of human subjects in federally sponsored research. GINA prohibits collection of and reliance on genetic information in specified circumstances related to health insurance and employment.

Outside of the health sector, a "consumer protection" model dominates U.S. privacy law.[20] The consumer protection model provides a system of negative rights — data collection and processing are generally allowed unless a practice is specifically banned. These laws also tend to assume a commercial relationship between the data subject and the organization collecting or processing data. Most U.S. statutes (although not all, as we shall see, particularly in the health sector) fall within the frame of consumer protection.

The "data protection" model dominant in other countries — and in U.S. health privacy law — is more restrictive than the consumer protection model. Data protection laws generally ban collection and processing of personal data unless explicitly permitted. The data protection model is founded on the notion that privacy rights over personal information are inherent human rights, regardless of the nature of the transaction involved.[21] Accordingly, regulations developed under the data protection model provide affirmative individual rights. Under data protection laws such as the European Union's GDPR, individuals must consent to collection, use, or further distribution of personal data in many cases, and they also have the right of access to the data and ongoing rights to demand correction or deletion of information in many circumstances. Data protection laws also tend to be omnibus statutes enforced by a single national data protection regulator across all sectors, including government, nonprofit organizations, private companies — and health care institutions involved in either clinical care or research.

The closest thing the U.S. has to a broad-based privacy regulator like those in other countries is the Federal Trade Commission (FTC). Exercising its consumer protection powers under Section 5 of the Federal Trade Commission Act, the FTC serves as a backstop to narrowly tailored sectoral privacy laws. Section 5 authorizes the FTC to bring enforcement actions against "unfair and deceptive acts or practices" in interstate commerce. Thus, the FTC may institute an enforcement action when a business fails to implement or maintain reasonable privacy and security practices. Deceptive acts or practices occur when an entity makes misleading statements about its activities, such as when it violates its own privacy policies or other public comments concerning its handling of personal data. When alleging unfairness actions, the FTC must satisfy a three-prong test and allege that the practice: "(1) causes or is likely to cause substantial injury to consumers (2) which is not reasonably avoidable by consumers themselves and (3) [is] not outweighed by countervailing benefits to consumer or to competition."[22]

There are limits on the FTC's enforcement authority. First, the Commission's authority under the FTC Act applies only to matters "in or affecting commerce" by companies that are "organized to carry on business for [their] own profit or that of [their] members."[23] Thus, the Commission does not have enforcement authority over government entities or most legitimate non-profit organizations. Additionally, the jurisdictional scope is subject to certain sector specific exemptions, such as banks and common carriers.[24] Aside from these carveouts, however, the Commission has rather sweeping authority to pursue enforcement actions against unfair and deceptive acts or practices. As a result, while certainly not the same as a data protection regulator in other countries, the FTC does exercise oversight over handling of personal data in a broad swath of American institutions. Importantly here, the healthcare sector and health information are within the scope of the Commission's enforcement authority, and the FTC has brought actions against health care entities for Section 5 violations.[25]

Second, the FTC ordinarily cannot seek financial penalties against first-time offenders for direct Section 5 violations in privacy cases.[26] Rather, the FTC will negotiate a consent decree with the subject that binds it to certain compliance measures for typically twenty years. Then, if the FTC determines that a company has violated the terms of its consent decree, the FTC can seek to impose significant financial fines for the consent decree violation. For example, the FTC's recent privacy and data security settlement order of Facebook is enforcing a 2012 consent decree previously reached

The Journal of Law, Medicine & Ethics, 48 (2020): 142-150. © 2020 The Author(s)

with the company, in addition to Section 5 itself.[27] This differs from the regulatory penalties under health and genetic privacy laws: HIPAA includes potential civil and criminal penalties on a first offense; the Common Rule authorizes the Office of Human Research Protections to terminate an entity's Institutional Review Board registration, which is likely to result in a loss of research funding; and GINA authorizes civil penalties (and in some cases private lawsuits against employers who violate the Act's employment protections).

Every state also has some form of general consumer protection law, commonly known as Unfair and Deceptive Acts or Practices (UDAP) statutes, although they vary in scope and strength from state to state.[28] These statutes typically echo the FTC's prohibitions of unfair and deceptive practices, and they generally empower state attorneys general to seek civil penalties, injunctive relief, and attorneys' fees and costs.[29] Many authorize individual and class action lawsuits as well. A few other state laws, such as the Illinois Biometric Information Privacy Act, impose additional restrictions on narrower classes of personal information, potentially including genetic data.

A new wave of privacy proposals at the state level seek to move somewhat beyond existing consumer protection laws such as UDAP statutes. The most prominent of these is the California Consumer Privacy Act (CCPA), which was signed into law in June 2018 and will take effect in 2020. Once in force, it will be the most stringent and expansive general privacy law in the U.S. The CCPA applies to any business that processes the "personal information" of California residents if the business exceeds one of three thresholds concerning size (earning more than $25 million gross revenue annually), volume of personal data (handling personal information concerning 50,000 or more consumers, households, or devices annually for commercial purposes), or primary function as a data broker (deriving fifty percent or more of its annual revenues from selling personal information). While these definitions will exclude many entities handling genetic and genomic information, it also could include many, especially private companies.

The CCPA has prompted similar bills at the state and federal level. Such measures were debated in over a dozen states in the last year, and a number of other states formed task forces to explore similar bills. For example, right after the CCPA was enacted a very similar bill was introduced in the New Jersey legislature.[30] This bill explicitly creates a right to opt out from third-party data sales, and it mandates disclosures about data handling practices. A CCPA-like bill passed through the Washington State Senate by a bipartisan vote in 2019 before dying in the lower house.[31] At the federal level, bills introduced in both houses of Congress have resembled the broad rights and requirements imposed by the GDPR and the CCPA. For example, Representative Suzan DelBene (D-WA) introduced a proposal that would mandate opt-in consent for the collection, storage, processing, or transfer of "sensitive" data — explicitly calling out genetic data is as a type of sensitive personal information.[32] These are just a few examples of many legislative attempts demonstrating a trend to broaden the U.S. privacy framework beyond the sectoral approach. Many of these broad privacy statutes contain carveouts to exclude health care entities, but as discussed further below, the scope and effectiveness of such exemptions vary.

Another trend present in recently enacted and proposed general privacy laws is a shift toward a broader definition of personal data. The GDPR, for one, includes not only information that specifically identifies a person but also any information that renders that person "identifiable." The GDPR directs covered entities to make the determination of whether a person is identifiable by taking account of "all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly." Expanding this definition even more, the CCPA includes all 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."[33] This further includes inferences that may be drawn from any "personal information" to create a profile about a consumer. The California Legislature has considered proposals to narrow the CCPA's definition of personal information, but as of this writing almost all of its broad language remains intact.[34] The New Jersey bill noted above echoes the CCPA's expansive definition of personal information.[35] Applying even more broadly, the Washington Privacy Act would cover "any information that is linked or reasonably linkable to an identified or identifiable natural person" that had not been deidentified or made publicly available.[36] These examples are just a few of many demonstrating a trend to expand the definition of personal information beyond the narrow view of personally identifiable information found in older statutes.

II. How General Laws Treat Genomic Data

While not narrowly tailored to address the health sector or genomics specifically, the laws discussed above cast a wide net, potentially encompassing the collection and processing of genetic data, even if they do not do so explicitly (or even intentionally at times). This part addresses such laws' treatment of genetic data

The Journal of Law, Medicine & Ethics, 48 (2020): 142-150. © 2020 The Author(s)

and considers scenarios in which the general-purpose privacy laws may apply to translational genomics.

General Data Protection Regulation

The GDPR governs any organization in the world that processes the personal data of any person based in the European Union and either monitors the behaviors of individuals located within the EU or offers goods or services to individuals in the EU. Thus, the applicability of the GDPR is determined by the status of the "data subject" — the individual about whom information is processed. The coverage of HIPAA, by contrast, is organization-centric, determined by the status of the entity doing the collecting or processing. The GDPR's broad definition of personal information explicitly includes a person's genetic information as an identifiable factor. Thus, the GDPR regulates a wider range of both entities and information than does HIPAA.[37]

The GDPR defines genetic information as "personal data relating to the inherited or acquired genetic characteristics of a natural person which result from the analysis of a biological sample from the natural person in question, in particular chromosomal, deoxyribonucleic acid (DNA) or ribonucleic acid (RNA) analysis, or from the analysis of another element enabling equivalent information to be obtained."[38] The GDPR includes genetic data in the special category of "sensitive data" subject to processing restrictions stricter than its already strict baseline. The GDPR generally prohibits processing of any genetic data unless it falls within an enumerated set of exemptions, including when the data subject has given explicit consent to the processing, the processing is necessary to protect the vital interests of the data subject, or the processing relates to personal data that are manifestly made public by the data subject.[39]

These consent requirements are strict. The GDPR already requires that consent to process ordinary personal data must be voluntary, freely given, specific, informed and unambiguous.[40] This is more exacting than the consent requirements under U.S. laws such as HIPAA or the Common Rule.[41] But for sensitive data, which includes genetic data, the GDPR is more demanding still, because consent must also be "explicit." The GDPR does not define "explicit" consent, but guidance published by a key EU advisory body listed several examples of sufficiently "explicit" consent, such as a hand-written signature, two-stage verification of consent, or an electronic signature.[42] The GPDR places the burden of proof of valid consent on the entity responsible for data processing.[43]

Because of the GDPR's broad jurisdictional sweep and limited exemptions, any actor that processes the genetic information of EU data subjects must meticulously evaluate its GDPR risk and compliance. For example, if an actor otherwise covered by HIPAA offers goods or services to individuals in the EU or monitors their behavior, it will be subject to the GDPR as either a "controller" or a "processor." This may be so even for an entity located solely in the United States. There are many efforts, such as one by the Global Alliance for Genomics and Health (GA4GH), to provide U.S. entities with information and facilitate harmonization between the GDPR and U.S. law. But even more than prior EU data protection law, the GDPR makes it clear that U.S. entities cannot focus only on the health-specific privacy law with which they have generally become most familiar.

Federal Trade Commission Act and Similar State Laws

The FTC's broad authority to pursue enforcement actions against "unfair and deceptive acts or practices" in interstate commerce overlaps with HIPAA enforcement actions brought by the Office of Civil Rights (OCR) within the Department of Health and Human Services (HHS). Thus, a HIPAA-covered entity must ensure that the disclosure statements it issues are not only HIPAA-complaint but also are not communicating unfair or deceptive messages to the consumer.[44] Further, OCR has advised HIPAA-covered entities that information practices for commercial, non-treatment-related purposes must also comply with the FTC Act.[45] The FTC itself has specifically provided guidance to DTC genetic testing companies suggesting best practices for maintaining compliance with the FTC Act.[46]

Moreover, the FTC has coordinated enforcement efforts with HHS in the past. For example, the FTC and HHS brought a dual enforcement action against Rite Aid Corporation for its failure to protect its customers' sensitive health information.[47] The two agencies opened the coordinated investigation into Rite Aid following news reports that the company had been using open dumpsters to dispose of trash that contained customer and employee sensitive health information, such as pharmacy labels and job applications.[48] The FTC alleged that the company's representations about its security procedures were deceptive and that its security practices were unfair.[49] To resolve the matter, the company agreed to pay $1 million to HHS to settle its HIPAA violation claim and entered into a 20-year consent decree with the FTC requiring it to establish a comprehensive information security program, among other requirements.

Thus, above and beyond any requirements under HIPAA, organizations handling genetic data must ensure that all of their public representations and their commercial practices adhere to the FTC Act. This FTC

The Journal of Law, Medicine & Ethics, 48 (2020): 142-150. © 2020 The Author(s)

authority imposes regulation of genetic privacy on those that are not covered entities under HIPAA, but it also can expand duties owed by covered entities.

Like federal regulatory actions on which the FTC and HHS cooperate, state attorneys general also combine their authority under health-specific privacy laws with their general-purpose consumer protection powers. The HITECH Act, enacted in 2009, authorized state attorneys general to bring HIPAA enforcement actions.[50] Pursuant to this authority, state attorneys general across the country have brought HIPAA enforcement actions in conjunction with actions enforcing general state consumer protection and data privacy statutes. In 2018, the Massachusetts attorney general announced a settlement with a Massachusetts hospital over the loss of unencrypted backup computer tapes that contained personal health information of more than 1,500 people.[51] In addition to alleging HIPAA violations, the Massachusetts enforcement action also alleged that the hospital violated the state's UDAP law and the Massachusetts Data Security Law.[52] In another case, a group of twelve attorneys general joined to bring an enforcement action against a third-party provider that licenses a web-based electronic health record application.[53] This action alleged violations of the states' respective UDAP statutes, breach notification statutes, and personal information statutes, as well as HIPAA violations.[54]

Thus, it is increasingly inaccurate to focus too much on health privacy law as the main source of potential liability for many health-related entities, when they are subject to consumer protection actions from both federal and state regulators.

California Consumer Privacy Act

The CCPA treats genetic information as an aspect of the "biometric information" subcategory of its personal information definition. Thus, any genetic information that "can be used, singly or in combination with each other or with other identifying data, to establish individual identity" falls within the statute's scope.

The CCPA explicitly exempts protected health information collected or sold by a covered entity or business associate pursuant to HIPAA and information collected as part of a clinical trial subject to the Common Rule. Notwithstanding these exemptions, however, the breadth of the definition of personal information suggests that lots of other actors and practices that interact with genomic data could still fall within its scope.[55] Because HIPAA's Privacy Rule only applies to "covered entities" and "business associates," many organizations handling genomic data will not enjoy this categorical exemption from the CCPA, including many DTC firms, pharmaceutical companies, and health analytics businesses.[56] To complicate matters further, even covered entities enjoy the exemption only with respect to information defined as personal health information by HIPAA. Thus, healthcare companies that have traditionally operated squarely within HIPAA's scope may have aspects of their business that collect information beyond HIPAA-protected personal health information.

The CCPA's HIPAA exemption does not categorically exempt all operations related to personal data conducted by covered entities and business associates. Instead, it exempts covered entities and business associates only "to the extent the provider or covered entity maintains patient information in the same manner as medical information or protected health information." It focuses on the classification of the information at issue as opposed to the classification of the entity that is doing the collecting or processing.[57] Thus, an entity that engages in HIPAA-covered practices in certain areas of its business may have genetic information that it collects or processes elsewhere for other purposes; that particular practice falls outside of HIPAA's scope and thus outside the exemption from the CCPA.

In the insurance context raised earlier, if a hybridized insurance company's noncovered component offers life or disability insurance, the collection and use of genetic data would not fall within the HIPAA exemption and thus be subject to the CCPA's requirements. Moreover, if a company offers a direct-to-consumer version of a smartphone app that is not provided on behalf of a covered entity, it would not be subject to HIPAA and thus it would fall under the CCPA. Furthermore, in the clinical context, because the Common Rule does not automatically apply to all clinical trials, research trials that are not funded by one of the federal agencies that have adopted the Common Rule do not fall within the CCPA's Common Rule exemption and are thus subject to its obligations.[58] In these and other potential scenarios, organizations involved in translational genomics may find that general-purpose privacy laws apply to their activities even when they are accustomed to being regulated by specialty laws such as HIPAA or the Common Rule.

Additionally, information can readily pass back and forth between the various regulatory schemes, both traditional and new. For example, genetic information that originated as personal health information subject to HIPAA's requirements can pass out of that regulatory bubble when disclosed outside of HIPAA's domain of covered entities. And the reverse is also true. Previously unregulated data that passes from an entity outside of HIPAA's scope becomes HIPAA-regulated personal health information in the hands of a covered entity, but retains its unregulated status with

The Journal of Law, Medicine & Ethics, 48 (2020): 142-150. © 2020 The Author(s)

the originator.[59] For example, if consumer data were collected by a business associate and merged with PHI indicators as part of a records system serving translational genomics, the new data comes under HIPAA when combined but falls outside it when maintained separately from its designated record set, even if held by the same entity. The porousness of the traditional laws regulating the health care sector emphasizes the importance of looking beyond the bubble of genetic privacy law to a new generation of more general privacy laws.

Conclusion

Traditionally, entities interacting with genetic data either through clinical work or research have evaluated the privacy regulatory landscape primarily through the lens of HIPAA, GINA, the Common Rule, and state genetic information laws. But, several recent trends suggest that this lens provides too narrow of a frame. First, the pool of actors now involved with genetic data is more diverse today than ever. Additionally, trends toward broadly applicable privacy laws such as the CCPA started to gain momentum in the United States. Finally, skepticism continues to grow concerning the adequacy of deidentification as a security tool in light of the unique characteristics of genetic data.

Beyond the traditional "health sector" perspective of genetic privacy law, any analysis of privacy risk in translational genomics must pay close attention to what genetic information is being gathered and from whom. In many circumstances, these activities could give rise to the restrictions and obligations of general-purpose privacy laws — the GDPR, FTC Act and corresponding state statutes, and CCPA to name a few. Furthermore, it is important for actors in this space to consider the characteristics and sources of the data. Any responsible overview of the laws applicable to genomics must look beyond those traditionally understood to govern the collection and processing of genetic data and consider a wider frame from which to assess regulatory compliance.

Note

The authors have no conflicts to declare.

References

1. L. Cartwright-Smith et al., "Health Information Ownership: Legal Theories and Policy Implications," *Vanderbilt Journal of Entertainment & Technology Law* 19 (2016): 207.
2. National Human Genome Research Institute, *Privacy in Genomics*, *available at* <https://www.genome.gov/about-genomics/policy-issues/Privacy> (last visited June 19, 2019); K. Norrgard, "Protecting Your Genetic Identity: GINA and HIPAA," *Nature Education* 1 (2008): 21, *available at* <https://www.nature.com/scitable/topicpage/protecting-your-genetic-identity-gina-and-hipaa-678> (last visited June 19, 2019); S. Fendrick, "The Role of Privacy Law in Genetic Research," *I/S: A Journal of Law and Policy for the Information Society* 4 (2008): 803, *available at* <https://kb.osu.edu/bitstream/handle/1811/72811/1/ISJLP_V4N3_803.pdf> (last visited February 4, 2020).
3. V. Gutmann Kocha and K. Todd, "Research Revolution or Status Quo?: The New Common Rule and Research Arising from Direct-To-Consumer Genetic Testing," *Houston Law Review* 56 (2018): 81.
4. M. Cech, "Genetic Privacy in the 'Big Biology' Era: The 'Autonomous' Human Subject," *Hastings Law Journal* 70 (2019): 851; P. Bailey, "Big Brother or Big Pharma: The Lion Fight Over the Surveillance and Promotion of Pharmaceutical Use in America," *Florida State University Law Review* 44 (2017): 1483.
5. S.D. Schilly and M.J. Khoury, "What Is Translational Genomics? An Expanded Research Agenda For Improving Individual and Population Health," *Applied Translational Genomics* 3, no. 4 (2014): 82–83, *available at* <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4694629/> (last visited February 4, 2020).
6. A. Regalado, "2017 Was the Year Consumer DNA Testing Blew Up," *MIT Technology Review* (2018), *available at* <https://www.technologyreview.com/s/610233/2017-was-the-year-consumer-dna-testing-blew-up/> (last visited June 19, 2019).
7. A. Regalado, "More than 26 Million People Have Taken an At-Home Ancestry Test," *MIT Technology Review* (2019), *available at* <https://www.technologyreview.com/s/612880/more-than-26-million-people-have-taken-an-at-home-ancestry-test/> (last visited October 6, 2019).
8. S. Zhang, "Big Pharma Would Like Your DNA," *The Atlantic*, July 27, 2018, *available at* <https://www.theatlantic.com/science/archive/2018/07/big-pharma-dna/566240/> (last visited February 4, 2020).
9. See, e.g., S. Zhang, "The Loopholes in the Law Prohibiting Genetic Discrimination," *The Atlantic*, March 13, 2017, *available at* <https://www.theatlantic.com/health/archive/2017/03/genetic-discrimination-law-gina/519216/> (last visited June 23, 2019).
10. C. J. Guerrini, J. O. Robinson, D. Petersen, and A. L. McGuire, "Should Police Have Access to Genetic Genealogy Databases? Capturing the Golden State Killer and Other Criminals Using a Controversial New Forensic Technique," *PLOS Biology* 16 (2018): 10, *available at* <https://doi.org/10.1371/journal.pbio.2006906> (last visited February 4, 2020).
11. P. M. Schwartz, "Preemption and Privacy," *Yale Law Journal* 118 (2009): 902.
12. See, e.g., Social Media Privacy Protection and Consumer Rights Act of 2019, S. 189, 116th Cong. (2019); Information Transparency & Personal Data Control Act, H.R. 2013, 116th Cong. (2019); "Consumer Data Privacy Legislation," *National Conference of State Legislatures* (2019), *available at* <http://www.ncsl.org/research/telecommunications-and-information-technology/consumer-data-privacy.aspx> (last visited October 6, 2019).
13. P. Ohm, "Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization," *UCLA Law Review* 57 (2010): 1701. See also C. Farr, "Facebook Sent a Doctor on a Secret Mission to Ask Hospitals to Share Patient Data," *CNBC* (2018), *available at* <https://www.cnbc.com/2018/04/05/facebook-building-8-explored-data-sharing-agreement-with-hospitals.html> (last visited June 19, 2019).
14. M.A. Rothstein, "Is Deidentification Sufficient to Protect Health Privacy in Research?" *The American Journal of Bioethics* 10 (2010): 3.
15. "Federal Policy for the Protection of Human Subjects," *Federal Register* 82, no. 12 (2017): 7149-7269, *available at* <https://www.govinfo.gov/content/pkg/FR-2017-01-19/pdf/2017-01058.pdf> (last visited February 4, 2020).
16. *Id.*
17. J. Riddle, "Final Rule Material: Secondary Research with Identifiable Information and Biospecimens," *Biomedi-*

The Journal of Law, Medicine & Ethics, 48 (2020): 142-150. © 2020 The Author(s)

cal Research Alliance of New York LLC (2017), *available at* <https://about.citiprogram.org/wp-content/uploads/2018/07/Final-Rule-Material-Secondary-Research-with-Identifiable-Information-and-Biospecimens.pdf> (last visited February 4, 2020); "KUMC Guidance Document for Exempt Research 2018 Common Rule Changes," University of Kansas Medical Center (2018), *available at* <http://www.kumc.edu/Documents/hrpp/Topical%20Guidance/KUMC%20Guidance%20Document%20for%20Exempt%20Research%202018%20Common%20Rule%20Changes.pdf> (last visited February 4, 2020).

18. *Id.*
19. W. McGeveran, *Privacy and Data Protection Law* (2016): 257-258.
20. W. McGeveran, "Friending the Privacy Regulators," *Arizona Law Review* 58 (2016): 973–975.
21. See Charter of Fundamental Human Rights of the European Union, Arts. 7 and 8; European Convention on Human Rights, Art. 8. See also *Google Spain SL v. AEPD*, Court of Justice of the European Union, 2014 E.C.R. 317.
22. 15 U.S.C. § 45(n).
23. *Id.* at § 45(a)(2) and 15 U.S.C. § 44.
24. *Id.* at § 45(a)(2).
25. See, e.g., In the matter of GeneLink, Inc. and Foru Corp., F.T.C. C-4456-4457 (2014), *available at* <https://www.ftc.gov/system/files/documents/cases/140512forutmcmpt.pdf> (last visited February 4, 2020); In the Matter of PaymentsMD, LLC, 2015 FTC LEXIS 24 (2015), *available at* <https://www.ftc.gov/enforcement/cases-proceedings/132-3088/paymentsmd-llc-matter> (last visited February 4, 2020); HenrySchein Practice Solutions, Inc., F.T.C. No. 1423161 (2016) (consent order), *available at* <https://www.ftc.gov/system/files/documents/cases/160105scheinagreeorder.pdf> (last visited February 4, 2020); Accretive Health, F.T.C. No. C-4432 (2014) (consent order), *available at* <http://www.ftc.gov/system/files/documents/cases/140224accretivehealthdo.pdf> (last visited February 4, 2020).
26. C.J. Hoofnagle, *Federal Trade Commission Privacy Law and Policy* (2016): 113–114.
27. D. Bartz, "Facebook Facing 20-Year Consent Agreement after Privacy Lapses: Source," *Reuters*, May 13, 2019, *available at* <https://www.reuters.com/article/us-facebook-ftc/facebook-facing-20-year-consent-agreement-after-privacy-lapses-source-idUSKCN1SJ2C2> (last visited February 4, 2020). See also "FTC Approves Final Settlement With Facebook," *Federal Trade Commission*, August 10, 2012, *available at* <https://www.ftc.gov/news-events/press-releases/2012/08/ftc-approves-final-settlement-facebook> (last visited February 4, 2020).
28. C. Carter, "Consumer Protection in the States: A 50-State Evaluation of Unfair and Deceptive Practices Laws," *National Consumer Law Center Inc.* (2018), *available at* <https://www.nclc.org/images/pdf/udap/udap-report.pdf> (last visited February 4, 2020).
29. D. K. Citron, "The Privacy Policymaking of State Attorneys General," *Notre Dame Law Review* 92, no. 2 (2016): 754.
30. 2018 N.J. S.B. 2834, *available at* <https://www.njleg.state.nj.us/2018/Bills/S3000/2834_I1.pdf> (last visited February 4, 2020).
31. "Washington Privacy Act," 2019 WA S.B. 5376, *available at* <http://lawfilesext.leg.wa.gov/biennium/2019-20/Pdf/Bills/Senate%20Bills/5376-S2.pdf> (last visited February 4, 2020).
32. Information Transparency & Personal Data Control Act, H.R. 2013 (116th Cong. 2019).
33. Cal. Civ. Code § 140(o)(1).
34. Cal. Civ. Code § 140(o)(1).
35. 2018 N.J. S.B. 2834, *available at* <https://www.njleg.state.nj.us/2018/Bills/S3000/2834_I1.pdf> (last visited February 4, 2020).
36. Washington Privacy Act, *supra* note 31.
37. S. Baird, "GDPR Matchup: The Health Insurance Portability and Accountability Act," *International Association of Privacy Professionals* (2017), *available at* <https://iapp.org/news/a/gdpr-match-up-the-health-insurance-portability-and-accountability-act/> (last visited February 4, 2020).
38. GDPR, Recital 34, *available at* <https://gdpr-info.eu/recitals/no-34/> (last visited February 4, 2020).
39 GDPR, Article 9, *available at* <https://gdpr-info.eu/art-9-gdpr/> (last visited February 4, 2020); "Special category data," *Information Commissioner's Office*, *available at* <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/special-category-data/> (last visited February 4, 2020).
40. GDPR, Article 7, *available at* <https://gdpr-info.eu/art-7-gdpr/> (last visited February 4, 2020).
41. For the Common Rule's "informed consent" standard, see For the Common Rule, see Department of Health and Human Services (DHHS), "Protection of Human Subjects," 45 C.F.R. Part 46 § 116, *available at* <http://www.hhs.gov/ohrp/human-subjects/guidance/45cfr46.html> (last visited February 4, 2020).
42. "WP29 Guidelines on Consent," *International Association of Privacy Professionals* (2018), *available at* <https://iapp.org/resources/article/wp29-guidelines-on-consent/> (last visited February 4, 2020).
43. "Burden of Proof and Requirements for Consent," *available at* <https://gdpr-info.eu/recitals/no-42/> (last visted February 4, 2020).
44. "Sharing Consumer Health Information? Look to HIPAA and the FTC Act," *Federal Trade Commission* (2016), *available at* https://www.ftc.gov/tips-advice/business-center/guidance/sharing-consumer-health-information-look-hipaa-ftc-act (last visited February 4, 2020).
45. S. Sheber, "OCR Releases Guidance for HIPAA-Covered Entities to Follow FTC Regulations When Sharing Patient Data," *Journal of AHIMA*, October 27, 2016, *available at* <https://journal.ahima.org/2016/10/27/ocr-releases-guidance-for-hipaa-covered-entities-to-follow-ftc-regulations-when-sharing-patient-data/>.
46. E. Jillson, "Selling genetic testing kits? Read on." *Federal Trade Commission* (2019), *available at* <https://www.ftc.gov/news-events/blogs/business-blog/2019/03/selling-genetic-testing-kits-read> (last visited February 4, 2020). See also L. A. Malek and J. E. Johnson, "Genetic Testing Is On FTC's Radar," *Law360*, April 18, 2019.
47. In the Matter of Rite Aid Corp., F.T.C. C-4308 (2010) *available at* <https://www.ftc.gov/sites/default/files/documents/cases/2010/11/101122riteaidcmpt.pdf> (last visited February 2, 2020). See also Press Release, "Rite Aid Settles FTC Charges That It Failed to Protect Medical and Financial Privacy of Customers and Employees," *Federal Trade Commission*, July 27, 2010, *available at* <https://www.ftc.gov/news-events/press-releases/2010/07/rite-aid-settles-ftc-charges-it-failed-protect-medical-financial> (last visited February 4, 2020).
48. *Id.*
49. Rite Aid Corp. complaint, *supra* note 47.
50. Health Information Technology for Economic and Clinical Health Act, Pub. Law No. 111-5, §§ 13001–424, 123 Stat. 226 (2009) (codified as amended at 42 U.S.C. §§ 300jj–300jj-51, 17901–53). See, e.g., *Commonwealth v. Beth Israel Deaconess Med. Ctr.*, Civ. No. 14-3627 (Mass. Sup. Ct. Nov. 20, 2014); *State v. Innova Hosp.*, No. 2010CI-13714 (Tex. Cty. Ct. Oct. 11, 2010); *State v. HealthNet*, Civ. No. 2:11-CV-16 (Vt. Dist. Ct. Jan. 14, 2011); Press Release, "Eye Care Retailer Settles in Data Security Lapse," *Office of the Attorney General of Maryland* (Aug. 19, 2015), *available at* <https://mdoag-public.sharepoint.com/press/2015/081915.pdf> (last visited March 24, 2020); Press Release, "A.G. Schneiderman Announces Settlement with University of Rochester to Prevent Future Patient Privacy Breaches," *Office of the Attorney General of New York*, December 2, 2015, *available at* <https://ag.ny.gov/press-release/2015/ag-schneiderman-announces-settlement-

The Journal of Law, Medicine & Ethics, 48 (2020): 142-150. © 2020 The Author(s)

university-rochester-prevent-future-patient> (last visited February 4, 2020).
51. Press Release, "McLean Hospital to Implement New Security and Training Programs After Data Breach Exposed Sensitive Health Information," *Office of the Attorney General of Massachusetts*, December 12, 2018, *available at* <https://www.mass.gov/news/mclean-hospital-to-implement-new-security-and-training-programs-after-data-breach-exposed> (last visited February 4, 2020).
52. *Id.*
53. Complaint, *States of Ariz. v. Med. Informatics Eng'g*, No. 3:18-cv-969-RLM-MGG, 2019 U.S. Dist. LEXIS 97107 (N.D. Ind. May 28, 2019), *available at* <https://images.law.com/contrib/content/uploads/documents/292/Indiana-Suit.pdf> (last visited February 4, 2020).
54. *Id.*
55. C. Dennis and E. Johnson, "Paging all health care privacy pros: CCPA deserves your attention despite HIPAA exemption," *International Association of Privacy Professionals*, July 25, 2018, *available at* <https://iapp.org/news/a/paging-all-health-care-privacy-pros-cacpa-deserves-your-attention-despite-hipaa-exemption/> (last visited February 4, 2020).
56. L. Linnea, "Transparency and Direct-to-Consumer Genetic Testing Companies," *Harvard Law Petrie-Flom Center*, November 22, 2016, *available at* <http://blog.petrieflom.law.harvard.edu/2016/11/22/transparency-and-direct-to-consumer-genetic-testing-companies/> (last visited February 2, 2020).
57. P. Pitts, "The Privacy Delusions Of Genetic Testing," *Forbes*, February 15, 2017, *available at* <https://www.forbes.com/sites/realspin/2017/02/15/the-privacy-delusions-of-genetic-testing/#670caf2e1bba> (last visited Febrary 4, 2020); D. Elfin, "DNA Testing? You Might Want to Wait for More Legal Protection," *Bloomberg Law*, January 7, 2019, *available at* <https://news.bloomberglaw.com/pharma-and-life-sciences/dna-testing-you-might-want-to-wait-for-more-legal-protection> (last visited February 4, 2020); C. Ornstein, "Privacy Not Included: Federal Law Lags Way Behind New Health-Care Technology," *Pacific Standard Magazine*, June 14, 2017, *available at* <https://psmag.com/social-justice/privacy-not-included-federal-law-lags-way-behind-new-health-care-technology> (last visited February 4, 2020).
58. S. Hoffman, "Electronic Health Records and Medical Big Data," *Cambridge Bioethics and Law* (2016): 131–134.
59. "Health Information Privacy Beyond HIPAA: A 2018 Environmental Scan of Major Trends and Challenges," *National Committee on Vital and Health Statistics*, December 13, 2017, *available at* <https://www.ncvhs.hhs.gov/wp-content/uploads/2018/02/NCVHS-Beyond-HIPAA_Report-Final-02-08-18.pdf> (last visited February 4, 2020).

The Journal of Law, Medicine & Ethics, 48 (2020): 142-150. © 2020 The Author(s)