Big Data, Surveillance Capitalism, and Precision Medicine: Challenges for Privacy

Currents in Contemporary Bioethics

Mark A. Rothstein

Keywords: HIPAA, Precision Medicine, Privacy, Social Media, Surveillance Capitalism

Abstract: Surveillance capitalism companies, such as Google and Facebook, have substantially increased the amount of information collected, analyzed, and monetized, including health information increasingly used in precision medicine research, thereby presenting great challenges for health privacy.

Introduction: Big Data and Modern Medicine

We live in the information age. Technological developments in recent decades have enabled the compilation, aggregation, and curation of vast amounts of data of every conceivable kind. The term "Big Data" is used to describe an important subset of this information, "a large collection of disparate data sets that, taken together, can be analyzed to find unusual trends."[1] Four key concepts are embodied in this brief definition. First, Big Data involves the acquisition of unprecedented amounts of information that have become available through digitization of already compiled data and the systematic collection of staggering amounts of new information. Second, Big Data often involves linking types of information that previously were rarely, if ever, considered together. Third, analysis of the data is facilitated by artificial intelligence, including various applications of machine learning. Fourth, continually updated algorithms are intended to produce unanticipated associations or trends. Because it is not known what diverse data may be valuable, Big Data requires extensive data collection, and therefore it proceeds on the assumption that more data are always good to collect.

Big Data's entry into medical practice has been accelerated by the widespread adoption of electronic health records (EHRs). Spurred on by $35 billion in federal financial assistance from the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009,[2] by 2015, 96 percent of hospitals[3] and 80 percent of physicians[4] had an EHR system certified by the Department of Health and Human Services. The next wave of development is the adoption of federal interoperability standards, which will facilitate data transfer and analytics that can span multiple health care systems.[5]

The compilation and analysis of personal data have been dominated by huge, highly profitable technology companies, such as Google and Facebook. Substantial revenue for these types of companies comes from the commercial value derived from detailed facts about individuals that document prior actions, predict future actions and risks, and can be used to nudge or encourage certain behaviors. Surveillance capitalism describes the various ways in which technology companies generate personal data through intrusive surveillance methods, use proprietary algorithms to analyze personal data, and monetize the data by selling it to a wide range of customers.

Some experts believe that Big Data will transform the practice of medicine,[6] although insights from Big Data are now used mostly in health research.[7] The federally sponsored

Mark A. Rothstein, J.D., *is the Herbert F. Boehl Chair of Law and Medicine, Director, Institute for Bioethics, Health Policy and Law, at the University of Louisville School of Medicine in Louisville, Kentucky, USA.*

About This Column

Mark A. Rothstein serves as the section editor for *Currents in Contemporary Ethics*. Professor Rothstein is the Herbert F. Boehl Chair of Law and Medicine and the Director of the Institute for Bioethics, Health Policy and Law at the University of Louisville School of Medicine in Kentucky. (mark.rothstein@louisville.edu)

The Journal of Law, Medicine & Ethics, 49 (2021): 666-676. © 2021 The Author(s)
DOI: https://doi.org/10.1017/jme.2021.91

and administered Precision Medicine Initiative is the most ambitious Big Data undertaking in health care. Its research protocol, the All of Us research program, is collecting vast amounts of data from diverse individuals for long-term research use. However, the acquisition, storage, analysis, use, and dissemination of prodigious amounts of health and other sensitive information raise significant privacy concerns, brought into stark relief by inadequate current laws.[8]

This article explores how Big Data technology and novel, aggressive business practices have led to the prominent role of surveillance capitalism. Furthermore, surveillance capitalism can be expected to play a substantial role in precision medicine in generating data for and expropriating the findings of precision medicine. The article concludes with a discussion of some essential elements that should be included in new health privacy legislation to provide stringent but reasonable protections.

Surveillance Capitalism

In her highly acclaimed and deeply disturbing book, *The Age of Surveillance Capitalism: The Fight for a Human Future at the Frontier of Power*, Shoshana Zuboff defines surveillance capitalism as "the unilateral claiming of private human experience as free raw material for translation into behavioral data."[9] She describes how the business models of technology companies such as Google are based on exploiting vast amounts of personal data. Zuboff quotes Larry Page, co-founder of Google: "People will generate enormous amounts of data … Everything you've ever heard or seen or experienced will become searchable. Your whole life will be searchable."[10] Eric Schmidt, former Chief Executive Officer of Google, similarly stated:

> You give us more information about you, about your friends, and we can improve the quality of our searches. We don't need you to type at all. We know where you are. We know where you've been. We can more or less know what you're thinking about.[11]

Why would billions of people[12] allow technology companies to appropriate their private information for data mining and sale to an undisclosed, vast array of interested parties? Zuboff suggests an answer. "Surveillance capitalism offers solutions to individuals in the form of social connection, access to information, time-saving convenience, and, too often, the illusion of support."[13] And all of these services are seemingly "free."

This article explores how Big Data technology and novel, aggressive business practices have led to the prominent role of surveillance capitalism. Furthermore, surveillance capitalism can be expected to play a substantial role in precision medicine in generating data for and expropriating the findings of precision medicine. The article concludes with a discussion of some essential elements that should be included in new health privacy legislation to provide stringent but reasonable protections.

Proprietary Algorithms

An initial concern about surveillance capitalism is that businesses using the internet have unfettered access to everyone's personal information for an unlimited time[14] and for good or nefarious purposes. But disparate data snippets, associations, and preferences are merely the raw materials for the black box algorithms of Google, Facebook, and other technology companies.[15] The technology companies do not merely compile data and sell personal information to commercial entities for targeted advertising and marketing. The value added and huge profits of surveillance capitalism are based on developing and using proprietary algorithms to continually update the digital profiles of billions of people — their characteristics, lifestyles, experiences, environments, interests, associations, wants, and beliefs. This allows the companies to *predict* individuals' likely behaviors, such as their interest in various products and services and the most effective way for commercial entities to exploit consumer profiles for financial gain.

Influencing Behavior

Even more troubling, comprehensive data collection and analytics can *influence* behavior through the ostensibly innocuous algorithms that order online search results and select the content for personalized news feeds.[16] Personal data about interests and attitudes also can be used to motivate actions, such as organizing and coordinating the activities of groups comprised of like-minded individuals regarding social, racial, political, religious, or other sensitive matters. Joining with others who share interests can be personally and socially beneficial, such as enabling individuals with certain health conditions to communicate with others with similar afflictions. Yet, manipulation of data and people raises increasingly troubling societal issues of privacy, autonomy, liberty, social cohesion, and democracy.

National Security, Politics, and Disinformation

There is an irony in invasive surveillance technology being used to

The Journal of Law, Medicine & Ethics, 49 (2021): 666-676. © 2021 The Author(s)

https://doi.org/10.1017/jme.2021.91 Published online by Cambridge University Press

undermine or even destabilize government. After the terrorist attacks of September 11, 2001, federal agencies responsible for intelligence gathering and national security solicited Google and other technology companies to accumulate vast troves of data on potentially violent individuals and groups. The connection between the technology companies and government security agencies was revealed by Edward Snowden in 2013,[17] but the simultaneous, ubiquitous, private surveillance by these companies makes the national security uses of surveillance capitalism less surprising and perhaps more inevitable than previously assumed.

Meanwhile, beginning with Barack Obama's 2008 presidential campaign, data analytics became an integral part of mainstream American politics. Targeted fundraising and voter appeals gave the Obama campaign an edge, thereby initiating an "arms race" in cyber campaigning. By 2012, Obama's reelection campaign, working with Eric Schmidt of Google, "knew every wavering voter in the country that it needed to persuade to vote for Obama, by name, address, race, sex, and income,"[18] to permit "micro-targeting" of campaign efforts. By 2016, these same techniques were utilized by both political parties at the federal and state levels, and by numerous political campaigns around the world, including the Brexit vote.[19] Also in 2016, Cambridge Analytica, a political data analytics firm, improperly obtained personal data from 87 million Facebook users to develop predictive voter profiles later used by the Trump campaign.[20]

Since then, the largely unregulated universe of data acquisition, aggregation, analytics, and application has been exploited by malevolent domestic and foreign operatives to launch disinformation campaigns.[21] It also facilitated diverse and dispersed individuals to coordinate and carry out violent acts, as epitomized by the insurrection at the U.S. Capitol on January 6, 2021.[22] Additionally, misinformation about COVID-19 distributed on social media has led to significant resistance to vaccination, masking, social distancing, and other public health measures, resulting in many thousands of preventable deaths and the prolongation of the worst pandemic in a century.[23]

New Sources of Data

To maintain their competitive advantage and to continue generating vast profits the largest technology companies have updated their predictive capabilities by exploiting new sources of data. The best example is Google. Through aggressive deployment of internally developed surveillance methods (e.g., Street View, Google Maps) and corporate acquisitions (e.g., YouTube, Fitbit), Google extended its data sources beyond internet searches to e-mails, texts, photos, songs, videos, locations, interests, faces, emotions, social networks, consumer activity, smart home devices, wearables, and health information.[24] The goal is ubiquitous data capture, intervention, action, and control of economic behavior.

Other technology giants followed Google's financially successful strategy of diversifying and expanding their sources of unique, personal data. For example, Facebook acquired Instagram, developed the Novi digital wallet, and harvested data from its Like button to get a more robust view of individuals' preferences and associations. Microsoft acquired LinkedIn to provide additional data that could be analyzed and marketed.[25] Internet service providers, including Verizon, AT&T, and Comcast, also began monetizing data derived from subscribers' internet activity. To launch these new ventures quickly, some companies with large customer bases acquired established technology companies, as exemplified by Verizon's purchase of Yahoo! and AOL.[26]

Internet of Things

Novel methods of surveillance capitalism generate new sources of data and new privacy concerns. This is especially the case with the "Internet of Things," which involves billions of networked sensors that record and transmit data over the internet,[27] producing additional raw materials for artificial intelligence. These data sources include medical devices; environmental sensors; surveillance in public spaces, including facial recognition; "smart" televisions and other entertainment systems; "smart" cars, buildings, homes, and clothing; and digital assistants that record and relay users' commands and other conversations.[28] Many consumers infatuated with the latest "smart" technology do not realize that detailed data may be continuously recorded and transmitted for analysis.[29]

An example of these privacy issues involves smart toys, which can recognize the voices of individual children and interact in a personal way for appropriate educational and entertainment purposes. These toys usually have external Bluetooth and Wi-Fi connections, which can disclose a child's location information and make the child vulnerable to harm.[30] In theory, parents who give these toys to their child implicitly or explicitly consent to data collection and transmission about their child, but they cannot consent to disclosures made by their child's playmates that may occur at the same time.[31] Lawsuits and regulatory actions dealing with smart toys include data breaches involving hundreds of thousands of passwords, user names, email addresses, and actual conversations children had with their dolls.[32]

The most notorious incident of a smart toy creating risks to young children and their families is Hello Barbie, which was introduced in 2015. The interactive Barbie doll was Wi-Fi enabled and could be hacked into a surveillance device for spying on children. It was also possible to hack the doll's system information and gain access to a family's Wi-Fi network, thereby enabling control of all internet-connected devices at the owner's home. Mattel, manufacturer of Hello Barbie, pulled the doll from the market.[33]

Medical Records

In 2019, the disclosure of Google's Project Nightingale, in partnership with Ascension, raised serious concerns about access to millions of medical records by Google. Ascension is a St. Louis-based, Catholic chain of 150

The Journal of Law, Medicine & Ethics, 49 (2021): 666-676. © 2021 The Author(s)

hospitals and 6,700 physicians, covering 50 million patients in 20 states and the District of Columbia. Without any notice to patients, consent, or even an opportunity to opt out, Ascension gave Google access to all of Ascension's complete, individually identifiable, EHRs.[34] The stated purpose was to use artificial intelligence to identify ways of improving patient outcomes.

After Project Nightingale was disclosed in the media, the first question many patients asked was whether this arrangement was legal under the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule, and the short answer is yes. As described below, covered entities under HIPAA, including health care providers, are permitted to use and disclose "protected health information" (individually identifiable information) without notice or consent for treatment, payment, or health care operations.[35] Quality improvement, the avowed purpose of Project Nightingale, is included in the definition of health care operations.[36] Since Ascension was permitted to do this analysis under HIPAA, Google, a "business associate" of Ascension, also could undertake the analysis on Ascension's behalf because the parties executed a business associate agreement.[37]

Unsurprisingly, Project Nightingale is not a "one off" arrangement of Google and Ascension. Other large technology companies, including Amazon, Apple, and Microsoft, have actively pursued research arrangements with some of the largest and most respected medical institutions in the country.[38] Even assuming there will be insights leading to improved health care, questions remain about whether health privacy and security will be maintained and whether it is acceptable to use millions of individually identifiable patient records for analysis and commercialization without notice to or consent from patients.

Using Surveillance Data to Predict and Control Risks

Predictive data are increasingly being used in common consumer activities. For example, most auto accidents are caused by careless acts, such as speeding, tailgating, running red lights, unsafe lane changing, and driving in bad weather.[39] Drivers involved in these accidents are more likely to be distracted, intoxicated, or teenaged.[40] Sensors installed in cars can measure how someone is driving, and some insurance companies believe that predictive information of driver behavior generated by sensors can reduce auto accidents and insurers' liability. A few years ago, my insurance agent offered me a discount on my auto insurance if I would allow placement of a sensor on my car to monitor how I drive.[41] I declined the discount and said I would pay what amounts to a "privacy tax" not to be monitored. However, drivers might not have this option much longer, as auto insurance is highly competitive, and companies requiring the use of sensors might be able to offer less costly auto insurance.[42]

Closely related, rental car companies could begin using sensors to monitor how their cars are being driven and then prevent their cars from being started if the driver has been careless or reckless.[43] Car rental companies could even base their driving predictions on sensor data of destinations, identity of occupants, and even the private conversations of passengers. Such surveillance measures probably would be legal under the weak version of consent in the United States in which consent is valid if individuals merely click "I agree" at the end of a multi-page document that virtually nobody reads.

Predictive analytics are also used to "encourage" individuals to make positive behavioral changes. For example, several years ago, my university-employer, like most large employers, began offering all employees a discount on their employee contributions for health insurance if we enrolled in an employer-sponsored and third-party administered wellness program involving self-reports on various health measures, such as weight, exercise, smoking, and alcohol consumption. I declined and chose to pay the "privacy tax." Lower paid employees at my university, such as housekeeping and cafeteria workers, could not afford to forego an increase in their take home pay and therefore enrolled in the wellness program and have been monitored and urged to achieve certain health goals.

Few would object to encouraging individuals to adopt healthier lifestyles, but the evidence is mixed, at best, that employer-sponsored wellness programs are effective in improving employee health, reducing health costs, or producing a positive return on investment.[44] Moreover, it is questionable whether any modest gains in wellness are worth the price of permitting employers to control health care costs by contracting with third-party companies to surveil employees' lifestyles and "encourage" health-promoting behavioral changes.

The examples of auto and health insurance only begin to scratch the surface of predictive analytics based on personal data harvesting. Other insurance products (e.g., life, disability, long-term care, and property and casualty) are among the next likely targets. Financial applications include consumer credit and home mortgages in which predictive analytics could consider consumers' purchasing history, credit card usage, and credit scores. Employment, education, and government uses are other likely applications. In these and other areas the two main issues are whether the algorithmic predictions are accurate and, if so, whether the insights they provide are worth the privacy incursions and other social costs.

Precision Medicine

At least since the Human Genome Project (1990-2003), the National Institutes of Health (NIH) has embraced large-scale research projects, such as the current Cancer Moonshot[45] and Brain Initiative.[46] NIH's large-scale precision medicine research project is called All of Us.[47] Precision medicine has been defined as an approach for protecting health and treating disease that takes into account a person's genes, behaviors, and environment.[48] Precision medicine has proven to be valuable in clin-

The Journal of Law, Medicine & Ethics, 49 (2021): 666-676. © 2021 The Author(s)

ical settings for treating various cancers and rare disorders, as well as for identifying the safest and most efficacious drugs for specific individuals.[49]

More widespread introduction of precision medicine into clinical settings depends on research developments, and this is where NIH is playing a leading role. The All of Us Research Program was begun in 2015, and in 2018 it began enrolling at least one million diverse individuals in the United States.[50] In addition to genome sequencing, All of Us participants are asked to share data from (1) health surveys (demographic, lifestyle, and substance use); (2) physical measurements (blood pressure, heart rate, weight, height, and body-mass index); (3) biospecimens (blood and urine); (4) EHRs (including medications, laboratory results, vital signs, and billing codes); (5) digital health (from Fitbit and other wearables); and (6) geospatial and environmental data (including weather, air pollution, and sensor readings).[51] The last two categories of data are especially relevant to surveillance capitalism.

Even though the All of Us Research Program is collecting an unprecedented volume of health data, it is not collecting all the data that could affect an individual's health. Additional precision medicine research and clinical applications also could include the following data fields: (1) health histories and vital statistics of family members, including birth and death certificates; (2) military service records, including health records and data on hazardous exposures; (3) employment records, including exposure and biological monitoring data: (4) financial information, including consumer data generated by credit cards and consumer loyalty programs; (5) educational records, including behavioral health information and student health service records; (6) travel information and geo-location data, including exposures; (7) social media postings, including behavioral and mental health self-reports; and (8) government records, including Social Security data, Veterans Administration health records, criminal justice information, professional licensure applications, drivers' license information, and passport information. What could emerge from virtually unlimited data collection would be health-based dossiers of incredible detail for algorithms to probe for associations, interpretations, and predictions.[52]

Precision medicine faces significant challenges. In addition to the scientific obstacles of demonstrating clinical utility in various settings, precision medicine has generated vigorous ethical and policy criticisms.[53] These include the argument that precision medicine, by developing individually tailored and therefore more expensive diagnostics and therapeutics, will exacerbate health inequities; that numerous predictions of slightly increased risks will create a population of "worried well" people; and that health system budgets for costly medical interventions providing only slightly improved outcomes could be better spent elsewhere.[54] Perhaps the greatest legal and ethical challenge would be protecting privacy if health records contained increasingly voluminous quantities of sensitive information that go beyond traditional medical information to include social, behavioral, financial, and other data.[55]

Challenges to Privacy

The All of Us Research Program has pledged to protect the privacy and security of participants' information through deidentification, storage of information on protected computers, certificates of confidentiality, and other measures.[56] Even assuming that there are no breaches of security, it is easy to envision sensitive health information being widely disclosed to third parties. Under the All of Us guidelines, research participants have access to their own health information, including the predictive health assessments produced by algorithms developed by researchers.[57] If a participant is to benefit from this personalized information, the data must be uploaded or somehow incorporated into the participant's clinical EHR, where it can be used by the participant's health care providers. Many people in the United States do not realize that once health information becomes part of their clinical record it does not gain privacy protection; in fact, it becomes more vulnerable to disclosure.[58]

HIPAA Privacy Rule

Much of this misunderstanding is related to the erroneous assumption that the HIPAA Privacy Rule[59] is comprehensive and stringent. It is neither. First, the Privacy Rule only applies to health care providers, health plans, health clearinghouses, and their business associates.[60] It does not apply to, among other entities, insurance companies (other than health insurers), employers, schools, financial institutions, or technology companies. Second, the Privacy Rule is weakened by numerous, broadly worded exceptions. As mentioned earlier, a covered entity, such as a hospital, is free to use and disclose individually-identifiable health information without a patient's knowledge or consent for treatment, payment, and health care operations.[61] In addition, there are twelve public purpose exceptions that permit covered entities to disclose individually-identifiable health information without notice or consent: (1) where required by law; (2) for public health activities; (3) about victims of abuse, neglect, or domestic violence; (4) for health oversight activities; (5) for judicial and administrative proceedings; (6) for law enforcement; (7) about decedents; (8) for cadaveric organ, eye, or tissue donations; (9) for some types of research; (10) when there is a serious threat to health or safety; (11) for special government functions, including national security; and (12) for workers' compensation.[62]

In the context of precision medicine, the most important exception to the HIPAA Privacy Rule is consent (or authorization). Individuals have a right to access their own health records and to direct a covered entity to disclose some or all of the contents of their health records to any other person or entity.[63] This gives rise to "compelled authorizations," whereby individuals subject to economic leverage or legal compulsion can be required to provide their health records for a governmental or

The Journal of Law, Medicine & Ethics, 49 (2021): 666-676. © 2021 The Author(s)

commercial purpose, such as applying for employment, insurance (life, disability, and long-term care), Social Security disability, workers' compensation, veterans' benefits, and professional licensure. The best estimate is that there are at least 25 million compelled authorizations each year in the United States.[64]

In many cases, third parties can require the disclosure of complete health records, and even where the authorization is for more limited records, covered entities often find it easier to send complete records than engaging in the time-consuming and costly process of reviewing and redacting certain information. In the era of precision medicine, health records could contain sensitive information about matters ancillary to health status, such as relational, lifestyle, or financial data. Furthermore, once health records are received by an entity not subject to the HIPAA Privacy Rule (e.g., prospective employer), HIPAA does not limit redisclosure of the information to other individuals and entities.

Procedural and Substantive Privacy

Challenges to privacy can be divided into procedural and substantive issues. The United States, having failed to enact a broad privacy law in the 1970s when it was first considered,[65] has adopted the default position that data access practices by public and private entities are lawful unless they violate a specific statute or regulation.[66] In operation, notice and consent for access, use, and disclosure of private information, epitomized by online "click through" consent, is seriously deficient because the notice is rarely read or understood, and the consent is rarely informed or knowing. Even where notice is more informative and consent is more intentional, the process of compelled authorization, discussed above, is inherently coercive.

Compelled authorizations, permissible under the HIPAA Privacy Rule and other laws in the United States, are prohibited under the European Union's General Data Protection Regulation (GDPR).[67] Recital 32 defines consent in a much more stringent way than in the United States.

> Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of a data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means or an oral statement.[68]

Legislation protecting privacy should address a range of procedural issues, such as transparency, limiting disclosures to the minimum necessary information, limiting identifiability to the minimum necessary, limiting time for use and disclosure of data, and prohibiting the reidentification of individuals and the redisclosure of information. Many of these limitations already are part of the GDPR. In the United States, these types of reforms are necessary but insufficient to protect informational privacy.

Substantive privacy protections require an analysis of the lawful uses of information. For example, under the Americans with Disabilities Act (ADA),[69] after an employer extends a conditional offer of employment, the employer may condition employment on the satisfactory completion of a medical examination and a review of the individual's health records.[70] This is a reasonable requirement because many jobs involve strenuous physical exertion or exposure to hazardous environments. Nevertheless, neither the medical examination nor the health record review must be limited to matters directly related to the prospective employee's job duties, even though an employer may not rescind a conditional offer for medical reasons that are not job-related.[71] The substantive issue is what information an employer may lawfully use in deciding employability, such as whether it is permissible to refuse to employ an individual who is at greater risk of a future health problem.[72] Other substantive health privacy issues include what personal health information insurers may consider in deciding insurability[73] and what health information government agencies may consider in ruling on eligibility for benefits.[74]

Toward Reasonable, Effective Regulation

Legislative, regulatory, and other legal measures to curtail excessive disclosure or use of health information have been adopted at an extraordinarily slow pace and existing enactments are ineffective. Three reasons for this unacceptable situation come to mind: (1) technology changes more quickly than law; (2) surveillance capitalists include some of the largest and most powerful companies with well-financed cadres of lobbyists and lawyers; and (3) regulation of information implicates fundamental aspects of American society, such as First Amendment freedom of speech and freedom of contract. The following elements should be a part of any enactment to protect health privacy in the age of Big Data, surveillance capitalism, and precision medicine.

Comprehensive Health Privacy Legislation

Unlike the great majority of industrialized democracies, the United States lacks comprehensive health privacy legislation.[75] The HIPAA Privacy Rule was only intended to protect privacy in the payment chain of health care. It does not apply broadly and does not prohibit the redisclosure of health information received by non-covered entities. The Privacy Rule also lacks effective remedies and does not include a private right of action for aggrieved individuals to redress harms caused by unlawful privacy breaches.[76]

A few states have recently enacted privacy legislation of a general nature, beginning with the California Consumer Privacy Act,[77] which has been followed, so far, by Virginia[78] and Colorado.[79] Illinois enacted the nation's first biometric information privacy law,[80] followed by Texas,[81] Washington,[82] and California.[83] Although state legislatures have been termed the "laboratories of democracy,"[84] it simply takes too long to enact legislation on emerging tech-

The Journal of Law, Medicine & Ethics, 49 (2021): 666-676. © 2021 The Author(s)

nologies in a substantial number of states, and some states are unlikely ever to enact such legislation. For the foreseeable future, the small number of idiosyncratic state laws are likely to remain inconsistent and often indecipherable.

In contrast to the limited protections of federal and state laws, the GDPR categorically treats health data as sensitive and strictly protected. Article 9, section 1 prohibits the processing of "data concerning health,"[85] which could be construed as covering not only traditional clinical information, but the broad classes of data collected by precision medicine.[86] Following the GDPR model would mean comprehensive, consistent privacy legislation rather than categorical legislation separately dealing with educational, financial, health, and other types of information.[87]

Stringent Consent Requirements

The viability of consent has been destroyed by technology companies. Many millions — if not billions — of people now regard consent as a "click through" burden that is a worthless, time consuming, formalistic requirement before they can download an app or software update. The actual consent language is often part of a long, legalistic document in small type, which further ensures that virtually nobody reads it.[88] Some consent documents even grant app developers and technology companies an extraordinary license to invade privacy.[89] In addition, compelled authorization is a form of coercion, but it is not prohibited by the HIPAA Privacy Rule or any state law in the United States.

Big Data, surveillance capitalism, and precision medicine are all complicated and still evolving. When combined and applied in the context of health privacy, the three concepts become even more difficult to analyze or regulate. This article has argued that vital privacy interests are at stake at the intersection of Big Data, surveillance capitalism, and precision medicine. Furthermore, the speed at which vast amounts of personal data are being accumulated means that the negative consequences of the current, largely *laissez faire* approach are becoming more pronounced. Comprehensive, federal health privacy legislation should be enacted to, among other things, limit the use of compelled authorization consent, prohibit "click through" consent, and place substantive controls on the use of health information.

Limiting the Use of Data

There are two main ways of protecting health privacy: limiting access to data and limiting use of data. Limiting access to data may be considered a procedural strategy to keep certain entities from obtaining data. For example, under the Genetic Information Nondiscrimination Act (GINA),[90] it is unlawful for an employer to "request, require, or purchase genetic information with respect to an employee or a family member of an employee …"[91] In theory, if an employer or other entity does not have access to certain data, it cannot use the data to the detriment of the individual, and the individual's privacy is also protected. In the case of GINA, this approach is undermined by compelled authorization practices, because even though employers may not request genetic information, healthcare providers and other entities in possession of genetic information often fail to take the extraordinary steps to delete or redact genetic information when complying with an authorization.

By contrast, limiting the use of data does not explicitly prohibit access to data, although GINA prohibits both access to and discrimination based on genetic information.[92] Where only use is prohibited, no reasonable individual or entity would want access to data that cannot legally be used because it might expose them to legal liability.[93] Thus, even without explicit access restrictions, use limitations may be effective in protecting privacy indirectly. However, legislation prohibiting the use of data is more difficult to enact because it must address the substantive issues of how decisions about inclusion and exclusion (e.g., employability, insurability) are made by employers, insurers, and other data users.[94]

Conclusion

Big Data, surveillance capitalism, and precision medicine are all complicated and still evolving. When combined and applied in the context of health privacy, the three concepts become even more difficult to analyze or regulate.[95] This article has argued that vital privacy interests are at stake at the intersection of Big Data, surveillance capitalism, and precision medicine. Furthermore, the speed at which vast amounts of personal data are being accumulated means that the negative consequences of the current, largely *laissez faire* approach are becoming more pronounced. Comprehensive, federal health privacy legislation should be enacted to, among other things, limit the use of compelled authorization consent, prohibit "click through" consent, and place substantive controls on the use of health information.

The Journal of Law, Medicine & Ethics, 49 (2021): 666-676. © 2021 The Author(s)

https://doi.org/10.1017/jme.2021.91 Published online by Cambridge University Press

This article is an expanded and annotated version of a presentation for the Institute for Biomedical Ethics at the University of Basel, Switzerland, on August 24, 2021.

Acknowledgements

The author greatly appreciates the valuable input from Kyle Brothers, Laura Rothstein, and John Wilbanks. Mary E. Dyche, J.D. 2022, Louis D. Brandeis School of Law, University of Louisville, provided excellent research assistance.

Note

The author has no conflicts of interest to disclose.

References

1. J.D. Halamka, "Early Experiences with Big Data at an Academic Medical Center," *Health Affairs* 33, no. 7 (2014): 1132-1138, at 1132.
2. Pub. L. 111-5 (February 17, 2009), 42 U.S.C. § 300jj et seq.
3. Office of the National Coordinator for Health Information Technology, *Health IT Dashboard,* "Non-federal Acute Care Hospital Health IT Adoption and Use: State Rates of Non-federal Acute Care Hospital EHR Adoption, Health Information Exchange and Interoperability, and Patient Engagement (2015)," *available at* <https://www.healthit.gov/data/apps/non-federal-acute-care-hospital-health-it-adoption-and-use> (last visited July 21, 2021).
4. Office of the National Coordinator for Health Information Technology, *Health IT Dashboard,* "Office-based Physician Health IT Adoption: State Rates of Physician EHR Adoption, Health Information Exchange and Interoperability, and Patient Engagement (2015)," *available at* <https://dashboard.healthit.gov/apps/physician-health-it-adoption.php> (last visited July 21, 2021).
5. *See* Centers for Medicare and Medicaid Services, Department of Health and Human Services, Final Rule, 85 Fed. Reg. 25510-25640 (May 1, 2020). *See also* M.A. Rothstein and S.A. Tovino, "Privacy Risks of Interoperable Electronic Health Records: Segmentation of Sensitive Information Will Help," *Journal of Law, Medicine & Ethics* 47, no. 4 (2019): 771-777.
6. *See, e.g.,* E.J. Topol, *Deep Medicine: How Artificial Intelligence Can Make Healthcare Human Again* (New York: Basic Books, 2019); J. Couzin-Frankel, "Medicine Contends with How to Use Artificial Intelligence," *Science* 364, no. 6446 (2019): 1119-1120; E.J. Emanuel and R.M. Wachter, "Artificial Intelligence in Health Care: Will the Value Match the Hype?" *Journal of the American Medical Association* 321 no. 23 (2019): 2281-2282; E.J. Topol, "High-Performance Medicine: The Convergence of Human and Artificial Intelligence," *Nature Medicine* 25, no. 1 (2019): 44-56, doi: 10.1038/s4159-018-0300-7.
7. *See* S. Hoffman, *Electronic Health Records and Medical Big Data* (New York: Cambridge University Press, 2016); M.A. Rothstein, "Ethical Issues in Big Data Health Research," *Journal of Law, Medicine & Ethics* 43, no. 2 (2015): 425-429; E. Vayena and A. Blasimme, "Health Research with Big Data: Time for Systematic Oversight," *Journal of Law, Medicine & Ethics* 46, no. 1 (2018): 119-129.
8. *See generally* J. Lane et al., eds., *Privacy, Big Data, and the Public Good: Frameworks for Engagement* (New York, Cambridge University Press, 2014); S. Lohr, *Data-ism: The Revolution Transforming Decision Making, Consumer Behavior, and Almost Everything Else* (New York: HarperCollins, 2015); V. Mayer-Schönberger and K. Cukier, *Big Data: A Revolution That Will Transform How We Live, Work, and Think* (Boston: First Mariner Books, 2014); B. Schneider, *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World* (New York: Norton, 2015).
9. S. Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (New York: Public Affairs, 2019): at 8.
10. *Id.* at 98.
11. *Id.* at 498.
12. For example, according to Facebook, at the end of 2020, it had 2.8 billion monthly active users and 1.8 billion daily active users. *Facebook Revenue and Usage Statistics* (2021), *available at* <www.businessofapps.com/data/facebook-statistics> (last visited July 17, 2021).
13. Zuboff, *supra* note 9, at 383.
14. The right to be forgotten emerged from Europe as the right of a private person to have private information about the person removed from internet searches and other directories. It was adopted in the European Union's General Data Protection Regulation (GDPR). *See* R.C. Post, "Data Privacy and Dignitary Privacy: *Google Spain,* the Right to Be Forgotten, and the Construction of the Public Sphere," *Duke Law Journal* 67, no. 5 (2017-2018): 981-1072.
15. *See generally* F. Pasquale, *The Black Box Society: The Secret Algorithms that Control Money and Information* (Cambridge: Harvard University Press, 2015).
16. In a controversial study involving 689,003 Facebook users, one group of users was mostly exposed to positive messages in their news feeds and the other was exposed to mostly negative messages. There was a statistically significant, but small effect on the tone of the users' own postings. *See* A.D.I. Kramer et al., "Experimental Evidence of Massive-Scale Emotional Contagion through Social Networks," *Proceedings of the National Academy of Sciences* 111, no. 24 (2014): 8788-8790, *available at* <https://doi.org/10.1073/pnas.1320040111> (last visited October 27, 2021). The study was criticized because there was no external IRB review, no informed consent other than the general Facebook user agreement, and the study involved manipulation. *See* D. Hunter and N. Evans, "Facebook Emotional Contagion Experiment Controversy," *Research Ethics* 12, no. 1 (2016): 2-3, doi: 10.1177/174016115626341.
17. In 2013, Edward Snowden, a National Security Agency contractor, revealed the details of a massive surveillance program using commercially developed spyware that, once loaded on a device, can harvest data from emails, text messages, GPS data, and other sources and transmit the information to the attacker. *See generally* G. Greenwald, *No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State* (New York: Henry Holt, 2016).
18. J. Ruttenberg, "Data You Can Believe In: The Obama Campaign's Digital Masterminds Cash In," *New York Times*, June 20, 2013, *available at* <https://www.nytimes.com/2013/06/23/magazine/the-obama-campaigns-digital-masterminds-cash-in.html> (last visited July 18, 2021), quoted in Zuboff, *supra* note 9, at 123-124.
19. "The turmoil associated with the 2016 US and UK political disinformation campaigns on Facebook was a well-known problem that had disfigured elections and social discourse in Indonesia, the Philippines, Colombia, Germany, Spain, Italy, Chad, Uganda, Finland, Sweden, Holland, Estonia, and the Ukraine." *Id.* at 508.
20. *See* L.O. Gostin et al., "Health and Privacy in the Digital Age," *Journal of the American Medical Association* 320, no. 3 (2018): 233-234; J. Isaak and M.J. Hanna, "User Data Privacy: Facebook, Cambridge Analytica, and Privacy Protection," *Computer* 51, no. 8 (2018): 56-59.
21. *See* Y. Benkler, R. Faris, and H. Roberts, *Network Propaganda: Manipulation, Disinformation, and Radicalization in American Politics* (Oxford, UK: Oxford University Press, 2018).
22. *See* D. Mack, R. Mac, and K. Bensinger, "'If They Won't Hear Us, They Will Fear Us': How the Capitol Assault Was Planned on Facebook," *BuzzFeedNews*, January 21, 2021, *available at* <https://www.buzzfeednews.com/article/davidmack/how-us-capitol-insurrection-organized-facebook> (last visited July 29, 2021).
23. *See* D. Romer and K.H. Jamieson, "Conspiracy Theories as Barriers to

The Journal of Law, Medicine & Ethics, 49 (2021): 666-676. © 2021 The Author(s)

Controlling the Spread of COVID-19 in the U.S.," *Social Science and Medicine* 263 (2020): 113356. *See also* M. Fisher, "Disinformation for Hire, a Shadowy Industry, Is Booking Around the World," *New York Times*, July 26, 2021, at A8; S. Frenkel, "Disinformation Is Big Business for One Doctor," *New York Times*, July 25, 2021, at 1.

24. Zuboff, *supra* note 9, at 128.
25. *Id.* at 164.
26. *Id.* at 170.
27. *See generally* C. Maple, "Security and Privacy in the Internet of Things," *Journal of Cyber Policy* 2, no. 2 (2017): 155-184, *available at* <https://doi.org/10.1080/23738871.2017.1366536> (last visited August 27, 2021).
28. Zuboff, *supra* note 9, at 480.
29. *See* M. Adams, "Big Data and Individual Privacy in the Age of the Internet of Things," *Technology Innovation Management Review* 7, no. 6 (2017): 12-24.
30. Maple, *supra* note 27, at 74.
31. *Id.*
32. A. Elise, "Toy Company Settles Lawsuit after Kids' Information Hacked," WCVB Boston, January 10, 2018, *available at* <https://www.wcvb.com/article/toy-company-settles-lawsuit-after-kids-information-hacked/15049212≥ (last visited July 29, 2021).
33. *See* S. Gibbs, "Hackers Can Hijack Wi-Fi Hello Barbie to Spy on Your Children," *The Guardian*, November 25, 2015, *available at* <https://www.theguardian.com/technology/2015/nov/26/hackers-can-hijack-wi-fi-hello-barbie-to-spy-on-your-children> (last visited August 1, 2021).
34. *See* R. Copeland, D. Mattioli, and M. Evans, "Inside Google's Quest for Millions of Medical Records," *Wall Street Journal*, January 11, 2020, *available at* <https://www.wsj.com/articles/paging-dr-google-how-the-tech-giant-is-laying-claim-to-health-data-11578719700?reflink=desktopwebshare_permalink> (last visited July 20, 2021). It is debatable whether the arrangement was ethical. For example, it is questionable whether the records needed to be accessible in identifiable form. A technology company of Google's sophistication could have deidentified the records without sacrificing the research significance of the data. Furthermore, patients should have been informed of the goals, methods, and parties involved in Project Nightingale and given the opportunity to opt out of the program. With 50 million records, the loss of a small percentage would not be detrimental and if a substantial number of patients elected to opt out, perhaps it would have convinced Ascension that the promised ends of the research did not justify the means.
35. 45 C.F.R. § 164.502(a)(1)(ii).
36. 45 C.F.R. § 164.501 (the term health care operations, includes "conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines…").
37. 45 C.F.R. § 164.504(e).
38. Copeland, Mattioli, and Evans, *supra* note 34. *See Dinerstein v. Google, LLC*, 484 F. Supp.3d 561 (N.D. Ill. 2020) (dismissing class action for invasion of privacy and other causes of action arising from the University of Chicago Medical Center's providing Google with access to all patient health records for analysis).
39. *See* E.L. King, "Top 15 Causes of Car Accidents and How You Can Prevent Them," *HuffPost*, December 6, 2017, *available at* <https://www.huffingtonpost.com/laiza-king-/top-15-causes-of-car-accidents_b_11722196.html?ncid=engmodushpmg00000004> (last visited July 29, 2021).
40. *Id.*
41. The lack of tickets, accidents, or damage claims would seem to be the best evidence of safe driving.
42. On the other hand, sensors damaged in a car accident make it much more expensive to repair cars. *See* A. Davies, "New Safety Gizmos Are Making Car Insurance More Expensive," *Wired*, January 26, 2020, *available at* <https://www.wired.com/story/safety-gizmos-making-car-insurance-more-expensive/> (last visited August 1, 2021).
43. Ignition interlocks connected to breathalyzers long have been proposed to prevent drunk driving. *See National Highway Safety Administration, Ignition Interlocks — What You Need to Know* (2019), *available at* <https://www.nhtsa.gov/sites/nhtsa.gov/files/documents/ignitioninterlocks_811883_112619.pdf#:~:text=An%20ignition%20interlock%20is%20an%20after-market%20device%20installed,above%20a%20pre-set%20limit%20or%20set%20point%2C%202> (last visited July 17, 2021).
44. *See, e.g.*, J.M. Abraham, "Employer Wellness Programs – A Work in Progress," *Journal of the American Medical Association* 321, no. 15 (2019): 1462-1463.
45. National Cancer Institute, National Institutes of Health, Cancer Moonshot, *available at* <https://www.cancer.gov/research/key-initiatives/moonshot-cancer-initiative> (last visited July 18, 2021).
46. National Institutes of Health, What Is the Brain Initiative? *available at* <https://braininitiative.nih.gov/> (last visited July 18, 2021).
47. National Institutes of Health, All of Us Research Program, The Future of Health Begins with Us, *available at* <https://allofus.nih.gov/> (last visited July 18, 2021).
48. Centers for Disease Control and Prevention, Precision Health: Improving Health for Each and Every One of Us, *available at* <https://www.cdc.gov/genomics/about/precision_med.htm> (last visited July 18, 2021).
49. *See* F.S. Collins and H. Varmus, "A New Initiative on Precision Medicine," *New England Journal of Medicine* 372, no. 9 (2015): 793-795.
50. National Institutes of Health, All of Us Research Program Overview, *available at* <https://allofus.nih.gov/about/all-us-research-program-overview> (last visited July 18, 2021).
51. The All of Us Research Program Investigators, "The 'All of Us' Research Program," *New England Journal of Medicine* 381, no. 1 (2019): 668-676.
52. *See* W.N. Price II and I.G. Cohen, "Privacy in the Age of Medical Big Data," *Nature Medicine* 25, no. 1 (2019): 37-43; C.O. Schneble, B.S. Elger, and D.M. Shaw, "All Our Data Will Be Health Data One Day: The Need for Universal Data Protection and Comprehensive Consent," *Journal of Medical Internet Research* 22, no. 5 (2020): 1-8, *available at* <http://www.jmir.org/2020/5/e16879> (last visited Oct. 27, 2021) (mass linkage of non-health data could transform it into heath data); E. Vayenna and A. Blasimme, "Biomedical Big Data: New Models of Control on Access, Use and Governance," *Journal of Biomedical Inquiry* 14, no. 5 (2017): 501-513 (biomedical Big Data now includes environmental, lifestyle, and other data).
53. *See, e.g.*, M. Chowkwanyun, R. Bayer, and S. Galea, "'Precision' Public Health — Between Novelty and Hype," *New England Journal of Medicine* 379, no. 15 (2018): 1398-1400; J.P. Evans et al., "Deflating the Genome Bubble," *Science* 331, no. 6019 (2011): 861-862; H. ten Have and B. Gordjin, "Precision in Health Care," *Medicine, Health Care and Philosophy* 21 (2018): 441-442.
54. *See* M.A. Rothstein, "Structural Challenges of Precision Medicine," *Journal of Law, Medicine & Ethics* 45, no. 1 (2017): 274-279; M.A. Rothstein, "Some Lingering Concerns about the Precision Medicine Initiative," *Journal of Law, Medicine & Ethics* 44, no. 2 (2016): 520-525.
55. *See* J.H. Jain et al., "The Digital Phenotype," *Nature Biotechnology* 33, no. 5 (2015): 462-463 (discussing composite picture of digital data).
56. *See* All of Us Research Program, National Institutes of Health, Protecting Data and Privacy, *available at* <https://allofus.nih.gov/protecting-data-and-privacy> (last visited July 18, 2021).
57. *See* All of Us Research Program, National Institutes of Health, Core Values, *available at* <https://allofus.nih.gov/about/core-values> (last vis-

The Journal of Law, Medicine & Ethics, 49 (2021): 666-676. © 2021 The Author(s)

ited July 18, 2021) ("participants have access to their information").
58. Reportedly, prospective and current participants in All of Us are not informed about the risk of privacy caused by compelled disclosure of their "enhanced" health records. The same process threatens the privacy of individuals who use direct-to-consumer genetic testing and then have the results added to their health records.
59. 45 C.F.R. pts. 160, 162, 164.
60. 45 C.F.R. § 160.102.
61. A covered entity is merely required to mention the disclosures in its Notice of Privacy Practices. 45 C.F.R. § 164.520.
62. 45 C.F.R. § 1964.512.
63. 45 C.F.R. § 1964.524.
64. M.A. Rothstein and M.K. Talbott, "Compelled Disclosures of Health Records: Updated Estimates," *Journal of Law, Medicine & Ethics* 45, no. 1 (2017): 149-155.
65. For a discussion of early congressional proposals, *see* A.R. Miller, *The Assault on Privacy: Computers, Data Banks, and Dossiers* (Ann Arbor: University of Michigan Press, 1971): at 220-238. The Privacy Act of 1974, 5 U.S.C. § 552a, was enacted in response to the Watergate scandal, but it was limited to protections for information maintained by the federal government.
66. By contrast, under the European Union's General Data Protection Regulation (GDPR), access or use of personal data is illegal unless there is an express provision permitting it. European General Data Protection Regulation, *available at* <https://gdpr.eu/> (last visited July 22, 2021).
67. *Id.*
68. *Id.* Recital 32. On surveillance capitalism and the GDPR, *see* B. Aho and R. Duffield, "Beyond Surveillance Capitalism: Privacy, Regulation and Big Data in Europe and China," *Economy and Society* 49, no. 2 (2020): 187-212.
69. 42 U.S.C. §§ 12101-12213.
70. 42 U.S.C. § 12112(d)(3).
71. 42 U.S.C. § 12112(b)(6).
72. *See* M.A. Rothstein, "Predictive Health Information and Employment Discrimination under the ADA and GINA," *Journal of Law, Medicine & Ethics* 48, no. 3 (2020): 595-602.
73. *See, e.g.,* M.A. Rothstein, "Time to End the Use of Genetic Test Results in Life Insurance Underwriting," *Journal of Law, Medicine & Ethics* 46, no. 3 (2018): 794-801.
74. *See, e.g.,* B.B. Geiger et al., "Assessing Work Disability for Social Security Benefits: International Models for the Direct Assessment of Work Capacity," *Disability and Rehabilitation* 40, no. 24 (2018): 2962-2970.
75. *See* E.K. Cortez, ed., *Data Protection Around the World: Privacy Laws in Action* (The Hague: Springer, 2021).
76. A few states provide a cause of action. *See, e.g.,* Cal. Civ. Code § 56.36(b).
77. Cal. Civ. Code §§ 1798.100-1798.198 (2018). The law applies to for-profit entities that do business in California, that collect consumers' personal information, and that meet certain financial thresholds. The law does not apply to, among other exempt entities, covered entities and business associates regulated by the HIPAA Privacy Rule. The law provides for civil damages, civil penalties, injunctive or declaratory relief, and other relief that a court may deem appropriate. *See* M.A. Rothstein and S.A. Tovino, "California Takes the Lead on Data Privacy Law," *Hastings Center Report* 49, no. 5 (2019): 4-5.
78. Virginia Consumer Data Protection Act, H.B. 2307 (2021), applies to entities that conduct business in Virginia or produce products or services targeted to Virginia residents and that either control or process personal data of at least 100,000 consumers in a calendar year or control or process personal data of at least 25,000 consumers and derive at least 50% of gross revenues from the sale of personal data. Among the exemptions from the statute are entities subject to HIPAA.
79. Colorado Privacy Act, S.B. 21-190 (2021), applies coverage standards identical to Virginia. Although the law exempts certain controllers of health data, it does not exempt them completely, as in California and Virginia.
80. 740 Ill. Comp. Stat. Ann. 14/1 et seq. (2008). The law prohibits private entities from obtaining, using, or selling a person's biometric identifier or information without first obtaining the individual's written, informed consent. A "biometric identifier" means "a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry." Any person aggrieved by a violation of the act may recover from an entity that negligently violates any provision of the law, liquidated damages of $1,000 or actual damages, whichever is greater. If the violation is intentional or reckless, the liquidated damages are $5,000. Reasonable attorney fees and costs, and injunctive relief also are recoverable. *See Patel v. Facebook, Inc.*, 932 F.3d 1264 (9th Cir. 2019), cert. denied, 140 S. Ct. 937 (2020) (holding that class action status was proper in action challenging Facebook's "tag suggestions" photo feature); *Vance v. Microsoft Corp.*, 2021 WL 963485 (W.D. Wash. 2021) (action brought by Illinois residents alleging Microsoft downloaded and conducted facial scans of plaintiffs' photos without consent to improve its facial recognition technology).
81. Vernon's Tex. Bus. & Com. Code Ann. § 503.001 (violators subject to $25,000 civil penalty in action brought by state attorney general).
82. West's Wash. Rev. Code Ann. §§ 19.375.010 et seq. (act does not provide for a private right of action).
83. California's Consumer Privacy Act, *supra* note 77, includes "biometric information" within the definition of "personal information" protected by the statute, but damages are limited to $100 to $750 per violation if there is unauthorized access, theft, or disclosure because of a business' violation.
84. *See New State Ice Co. v. Liebmann*, 285 U.S. 262, 311 (1932) (Brandeis, J., dissenting) ("It is one of the happy accidents of the federal system that a single, courageous state, may, if its citizens choose, serve as a laboratory, and try novel social and economic experiments without risk to the rest of the country.").
85. "Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, *data concerning health* or data concerning a natural person's sex life or sexual orientation shall be prohibited." GDPR art. 9, § 1 (emphasis added).
86. *See* text accompanying notes 51-52 *supra.*
87. *See* N.P. Terry, "Big Data Proxies and Health Privacy Exceptionalism," *Health Matrix* 24, no. 1 (2014): 65-108.
88. *See* K. Litman-Navarro, "We Read 150 Privacy Policies. They Were an Incomprehensible Disaster," *New York Times,* June 12, 2019, *available at* <https://www.nytimes.com/interactive/2019/06/12/opinion/facebook-google-privacy-policies.html> (last visited August 1, 2021); *See also* A. Bruvere and V. Lovic, "Rethinking Informed Consent in the Context of Big Data," *Cambridge Journal of Science and Policy* 2, no. 2 (2021), doi.org/10.17863/CAM.68396.
89. In an assessment of the 36 top-ranked apps for depression and smoking cessation, 29 transmitted data for advertising and marketing purposes to Google and Facebook, but only 12 of 28 transmitting data to Google and 6 of 12 transmitting to Facebook disclosed this fact. K. Huckvale, J. Torous, and M.E. Larsen, "Assessment of Data Sharing and Privacy Practices of Smartphone Apps for Depression and Smoking Cessation," *JAMA Network Open* 2, no. 4 (2019): e192542. Also, in a study of 211 Android diabetes apps, permissions required to download the app authorized collection of tracking information (17.5%), activating the camera (11.4%), activating the microphone (3.8%), and modifying or deleting information (64.0%). S.R. Blenner et al., "Privacy Policies of Android Diabetes Apps and Sharing of Health Information," *Jour-*

The Journal of Law, Medicine & Ethics, 49 (2021): 666-676. © 2021 The Author(s)

nal of the American Medical Association 315, no. 10 (2016): 1051-1052.
90. 42 U.S.C. § 2000ff.
91. 42 U.S.C. § 2000ff-1(b).
92. 42 U.S.C. § 2000ff-1(a)
93. For example, Title VII of the Civil Rights Act of 1964, 42 U.S.C. §§ 2000e-2000e-17, does not prohibit employers from asking about the race of applicants and employees, but virtually no employers do so because inquiries about race might be offered as evidence of discrimination if a lawsuit were brought. *See* U.S. Equal Employment Opportunity Commission, Prohibited Employment Policies/Practices, *available at* <eeoc.gov/prohibited-employment-policiespractices> (last visited August 29, 2021).
94. *See* note 73 *supra*.
95. The possible regulation of surveillance technology companies by application of antitrust, consumer protection, or other laws is beyond the scope of this article.

The Journal of Law, Medicine & Ethics, 49 (2021): 666-676. © 2021 The Author(s)