Forthcoming in the Journal of Law, Medicine & Ethics
Vol. 48 (Supp. 1) (2020).

Unregulated Health Research Using Mobile Devices: Ethical Considerations and Policy Recommendations

Mark A. Rothstein
John T. Wilbanks
Laura M. Beskow
Kathleen M. Brelsford
Kyle B. Brothers
Megan Doerr
Barbara J. Evans
Catherine M. Hammack-Aviran
Michelle L. McGowan
Stacey A. Tovino

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

John T. Wilbanks is Chief Commons Officer of Sage Bionetworks.

Laura M. Beskow, M.P.H., Ph.D., is Professor and Ann Geddes Stahlman Chair in Medical Ethics at the Center for Biomedical Ethics and Society, Vanderbilt University Medical Center

Kathleen M. Brelsford, Ph.D., M.P.H., is Research Assistant Professor at the Center for Biomedical Ethics and Society, Vanderbilt University Medical Center.

Kyle B. Brothers, M.D., Ph.D. is Endowed Chair of Pediatric Clinical and Translational Research, University of Louisville School of Medicine.

Megan Doerr, M.S., L.G.C., is Principal Scientist, Governance at Sage Bionetworks.

Barbara J. Evans, J.D., Ph.D., is Mary Ann and Lawrence E. Faust Professor of Law, Professor of Electrical and Computer Engineering, and Director of the Center for Biotechnology and Law, University of Houston.

Catherine M. Hammack-Aviran, M.A., J.D., is Associate in Health Policy at the Center for Biomedical Ethics and Society, Vanderbilt University Medical Center.

Michelle L. McGowan, Ph.D., is Associate Professor, Department of Pediatrics and Department of Women's, Gender, and Sexuality Studies, Cincinnati Children's Hospital Medical Center.

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

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

Acknowledgements

The authors are indebted to the following members of the grant's working group, many of whom have written separate articles for this symposium or helped improve this article with their edits and comments: Kate Black, Shawneequa Callier, Ellen Wright Clayton, Ted Dove, Barbara Evans, Dov Fox, Malia Fullerton, Cindy Geoghegan, Aaron Goldenberg, Hank Greely, Christi Guerrini, Steve Hershman, Katie Huber, Marc Hurlbert, Eric Juengst, Bartha Maria Knoppers, Mary Majumder, Gary Marchant, Amy McGuire, Michelle Meyer, Camille Nebeker, Sally Okun, Pearl O'Rourke, Kevin Patrick, Patty Spears, Nic Terry, Sharon Terry, Jen Wagner, Susan Wolf, Joon-Ho Yu, and Ma'n Zawati.

This article deals with complex and contentious issues, and the views expressed do not necessarily represent the views of the people listed above. Indeed, all of the arguments and recommendations in the article do not necessarily represent the position of all authors.

Abstract

Mobile devices with health apps, direct-to-consumer genetic testing, crowd-sourced information, and other data sources have enabled research by new classes of researchers. Independent researchers, citizen scientists, patient-directed researchers, self-experimenters, and others are not covered by federal research regulations because they are not recipients of federal financial assistance or conducting research in anticipation of a submission to the FDA for approval of a new drug or medical device. This article addresses the difficult policy challenge of promoting the welfare and interests of research participants, as well as the public, in the absence of regulatory requirements and without discouraging independent, innovative scientific inquiry. The article recommends a series of measures, including education, consultation, transparency, self-governance, and regulation to strike the appropriate balance.

I. Background

A. Paradigm Shift in Health Research

Health research in the United States is undergoing a paradigm shift: broadening the ranks of health researchers and expanding the methods of health research. Part of this expansion involves the growth of "big data," the gathering and analyzing of vast troves of information about large numbers of people as a means to understand population health. Big data health research is an orienting focus of major federal and private research initiatives, including the Precision Medicine Initiative,[1] the Electronic Medical Records and Genomics Network,[2] and the Personal Genome Project.[3] This research often includes significant public engagement and greater involvement of human research participants, including an active role in planning and conducting the research itself.[4]

Big data and an expanded public role in research are cornerstones of citizen science, which may be defined as "a range of participatory models for involving non-professionals as collaborators in scientific research."[5] Citizen science includes enlisting non-experts in the collection, reporting, and analysis of health-related data; expanding health research from its traditional university- or industry-based settings through non-expert or public involvement in the conduct and governance of research; and crowdsourcing research to address specific population or community health needs.[6]

The growth of nontraditional health research sometimes blurs the line between professional and citizen science.[7] Nontraditional health researchers include, for example, independent researchers, citizen scientists, patient-directed researchers, do-it-yourself (DIY) researchers, and self-experimenters, and it is likely that new research arrangements and activities will be developed in the future.[8]

Several factors help to explain the appeal and growth of these new forms of health research.

1. Many people are critical of traditional health research, which they view as slow, expensive, unresponsive, and dominated by commercial interests.[9]

2. Crowdsourcing, N of 1 studies, and other alternative research methodologies have been excluded from traditional research funding mechanisms.[10]

3. The popularity and growth of social media and online patient communities facilitates collaboration, recruitment, participation, and dissemination of results.

4. The growth of DIY culture and the availability of direct-to-consumer (DTC) health-related (including genomic) testing has encouraged research by nonprofessionals.[11]

5. Public familiarity with digital health data and research platforms have demystified health research and made it seem similar to other forms of data analysis and consumer health technologies.

6. Smartphones with health apps and other mobile technologies have led to the collection of vast amounts of biometric data.

The potential of unregulated health research using mobile devices was on display in a groundbreaking study of Parkinson's disease in 2015. To take advantage of new software supporting health research on mobile devices, Sage Bionetworks, an independent nonprofit research organization based in Seattle,[12] conducted the first major smartphone-based health research study. The Parkinson's disease mPower study recruited participants online in partnership with collaborating Parkinson's disease organizations. The study used a novel, highly visual, self-guided, online consent process. Study data were generated by using the smartphone to record the voices of the participants, their posture and stability, their reaction time, and other measures of symptoms of Parkinson's disease. Approximately 17,000 participants, an unprecedented number, enrolled in the study over a six-month period. Although this study was not federally funded or

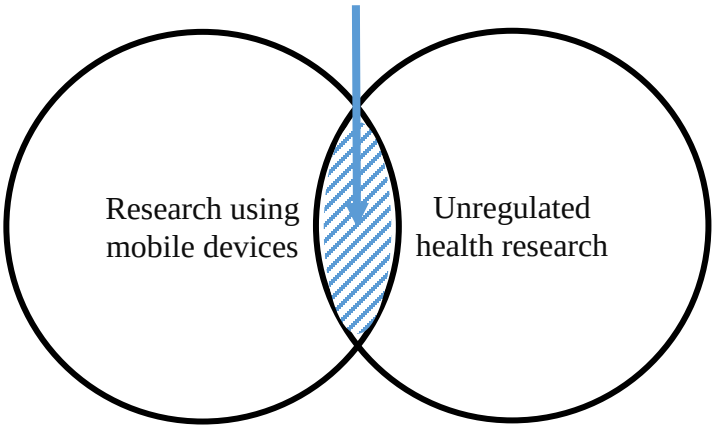
otherwise subject to regulation, including IRB review, the study protocol was submitted and approved by the WIRB-Copernicus Group, an independent IRB.

The new paradigm for health research challenges the regulatory requirements and research ethics norms that govern traditional approaches to human subject protections.[13] This new paradigm creates new tensions for research ethics and policy by disrupting the conventional definitions of health experts, funders, researchers, participants, and research settings. A fundamental question is whether it makes sense to apply a single set of regulations to research ethics with widely varying origins, methods, and funding sources.[14] Despite such challenges, the potential value of new research methods was recognized by Congress when it enacted the Crowdsourcing and Citizen Science Act of 2017.[15] That act grants federal agencies the authority to use crowdsourcing and citizen science in their research. In addition, the 21st Century Cures Act[16] directs the Food and Drug Administration (FDA) to create a trial framework to use "real world evidence" in its medical device oversight.[17]

This article reports the results of and builds upon a three-year study at the intersection of health research using mobile devices and unregulated health research.[18] The use of mobile devices in health research has increased significantly, and it is generally subject to the same regulations as other health research conducted by entities covered by the federal research regulations.[19] Unregulated health research uses various methods, including crowdsourcing information, DIY research, and N of 1 studies, which are beyond traditional health research. This article focuses on the intersection of these two important trends. See Figure 1.

Figure 1.

Unregulated Health Research Using Mobile Devices



Mobile devices and their health apps create new research risks based on significantly increased scale. By utilizing DTC genetic testing, publically accessible data repositories, biometric data collection and analysis, and other methods unregulated researchers can produce large-scale studies that raise concerns about balancing risks and benefits, informed consent, privacy, and other issues. Although these are traditional matters for researchers, participants, funders, and IRBs, unregulated health researchers largely operate by their own rules. This article reviews the benefits, risks, and policy alternatives to unregulated health research using mobile devices.

B. Unregulated Health Research and Researchers

The new health research described above is generally "unregulated" and conducted by "unregulated researchers."[20] As used in this article, "unregulated" means not subject to the federal regulations for the protection of human research subjects adopted by 16 federal departments and agencies ("Common Rule")[21] or promulgated by the Food and Drug Administration (FDA).[22] The research and researchers defined as "unregulated" may still be subject to other federal regulations. These include regulations on unfair or deceptive trade practices enforced by the Federal Trade Commission (FTC),[23] or the privacy, security, and breach notification rules promulgated under the

Health Insurance Portability and Accountability Act (HIPAA)[24] and the Health Information Technology for Economic and Clinical Health Act (HITECH Act).[25] "Unregulated" research and researchers also may be subject to regulation under state research laws or other state legislation.[26]

The definition of research used in this article follows the Common Rule definition, which provides in relevant part: "Research means a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge."[27] Similarly, the definition of "human subject" (or "participant" in this article) follows the Common Rule definition, which provides in relevant part: "Human subject means a living individual about whom an investigator (whether professional or student) conducting research: "(i) Obtains information or biospecimens through intervention or interaction with the individual, and uses, studies, or analyzes the information or biospecimens; or (ii) Obtains, uses, studies, analyzes, or generates identifiable private information or identifiable biospecimens."[28] Although research with deidentified specimens or data is not considered human subjects research under the Common Rule, our focus on unregulated research does not make such a distinction.

This article analyzes a wide range of unregulated health research with human participants, but it focuses on nontraditional and emerging types of researchers, such as independent researchers, citizen scientists, patient-directed researchers, and DIY researchers.[29] The context is health research using mobile devices. The article does not consider all possible unregulated researchers, such as corporations or foundations. Nor does it consider all forms of unregulated research that can affect human health, including environmental research,[30] citizen science gamification,[31] and citizen scientists and biohackers engaging in interventional clinical research and self-experimentation.[32] Although these issues are important, they are beyond the scope of this project.

C. Mobile Devices

The 2007 introduction of the iPhone permanently altered the long-term research landscape. It represented the replacement of devices that merely made phone calls with fully functional pocket computers that also made phone calls. The iPhone and all the other smartphones provided a design into which an increasing amount of hardware could be integrated, emulated in software, or attached to the phone via an app and network. According to recent estimates, 81% of North American adults own a smartphone,[33] and more than half of smartphone users are collecting "health-associated information" on their smartphones.[34] There are more than 325,000 mobile health apps available from the Apple App Store, Google Play Store, and other sources.[35]

Because of its direct connectivity, the smartphone creates unique research opportunities, such as the ability to pull and push information directly to and from the end user. It also allows developers to simplify complex processes, such as authorization to transfer data stored in online portals to secondary locations. Through ever-expanding hardware, smartphones increasingly contain sensors that can be repurposed from their initial use to surveil populations (e.g., GPS coordinates) and measure at least some elements of health (e.g., accelerometers). And via its connection to secondary mobile devices that tether with apps, a smartphone forms an expandable platform to connect app-navigated health devices and plug-ins, such as glucose meters, electrocardiograms, ultrasound, pulse oximetry, and heart rate monitors.[36]

Mobile devices with biometric measuring capabilities have obvious research implications. Smartphones facilitate access to hundreds of millions of potential research participants in the United States alone and can increasingly measure those participants in highly granular and personal ways. In 2015, Apple accelerated the role of smartphones in research by releasing an

open source toolkit called ResearchKit, which makes it easy to build mobile research applications.[37] A robust debate on the ethical, legal, and social implications of ResearchKit began shortly thereafter.[38] A companion open source Android toolkit called ResearchStack was released in 2016. No clear count of mobile research apps exists, but based on known implementations, more than thirty studies were launched in the first year of ResearchKit alone,[39] and a similar number of consents for mobile health apps were studied by the Global Alliance for Genomics and Health.[40]

Mobile devices intersect with a broader consumer technology market built on the integration of persistent behavior surveillance with advertising, with the smartphone deeply connected to the relevant business models.[41] Their apps represent controllable ways to interact with and monitor users. These apps can exploit many features of the phone in ways that consumers may not anticipate, like, or even understand.[42] In addition, the numerous uses of smartphones often create an information overload for consumers in looking at terms of service and privacy policies,[43] which are often written at levels that can baffle even graduate-level readers.[44] The common response of clicking "I agree" without carefully reading (or reading at all) the terms of service or privacy policies raises the issue of whether the consumer has provided valid consent to the uses described in these documents.[45]

Like other dominant sectors in consumer technology, mobile devices are characterized by a software monopoly. As of 2019, the vast majority of U.S. residents with smartphones used either Google or Apple app stores, with estimates as high as 99.74% using one of the two based on their choice of mobile operating system.[46] These two companies decide what apps are appropriate to maintain in their app stores, dictate requirements on what apps must and must not display to

consumers, and act to review and take down apps that violate their guidelines. They also possess the power to make or break an app based on, for example, how that app appears in searches, by placement on a featured page, or location within the app store.[47]

Apple and Google differ in hardware, however, as only an Apple phone runs an Apple operating system, and vice versa, whereas Google's Android is present on a dizzying variety of handsets. This allows Apple far more control over their hardware ecosystem. Apple leverages this to promote some privacy-supporting features;[48] Google's deep connection to advertising revenue means Android is by default a less protective of privacy.[49] They also differ in their approach to app stores; whereas Apple enforces a variety of community norms, Google takes a broad hands-off governance role.[50]

Apple and Google currently leverage existing software standards, such as SMART (Substitutable Medical Applications, Reusable Technologies) on FHIR (Fast Health Interoperability Resources), to enable access to health records by any healthcare provider with a compatible EHR system;[51] and the SMART on FHIR stack is broadly adopted by the emergent health data app community. Efforts around "consumer-led data transfer," such as the CARIN Alliance, have promulgated forms of normative community regulation through codes of conduct that can also be leveraged in regulatory thinking.[52]

D. Use Cases

As noted above, this analysis is designed to address scenarios that involve health research being conducted by unregulated researchers via mobile devices. This scope potentially includes a wide variety of scenarios, although there is no formal typology available to organize and reference specific types of scenarios. For this reason we have identified a set of use cases that will help

ground the sections that follow, including the discussion of ethical considerations (Part II) and the related policy recommendations (Part III). For definitional purposes, there are at least two characteristics of any study involving unregulated mobile health research: (1) whether the mobile health data were originally collected explicitly for research use, and (2) whether the data are being used for research purposes by the original collector/holder of the data.

The first factor is important because it determines whether app users are likely to understand that they are participants in a research study and not just users of an app. The fact that an app was created explicitly for a research purpose is also important because it points to the intention of the app developer or the organization funding the development of the app to serve as a researcher, thereby presenting additional expectations, such as informed consent. The second factor, whether an app is being used for research by the original collector, is important because the original collector of the data (typically the developer or funder of the app) has had direct contact with the app users and could thus be held responsible for ensuring the participant is informed of the research, has had an opportunity to give affirmative consent, etc. When research is conducted by a secondary recipient of the data, the lack of direct contact between the researcher and the participant means that the researcher is constrained in their ability to directly obtain consent, etc. Another important difference between the original data collected and the secondary recipient is that app use is typically not aware the secondary recipient has acquired their data.

These two criteria, original purpose of data collection and proximity of the research to the participant, can be used to form a 2 x 2 table (Table 1) containing four representative scenarios involving unregulated mobile health research. Although these four cells represent the general uses cases, it is important to examine a range of additional characteristics or variations of the four

scenarios that are also relevant to the ethical analyses and policy considerations addressed in this piece.

First, there are numerous types of unregulated researchers, including for-profit commercial companies, independent research organizations (i.e., not affiliated with academic or other institutions) (e.g., Sage Bionetworks), independent app developers, individual community/citizen scientists, patient-led groups (e.g., PatientsLikeMe), and individual and group self-experimenters (e.g., Crohnology).

Second, app users may include children or other individuals who lack capacity to make decisions regarding research participation and data inclusion. This presents additional issues, such as verifying the identity of the app user to ensure that any necessary consent is valid.[53]

Third, data used in unregulated research vary in sensitivity. For example, GPS data may increase the risk that de-identified data could be re-identified, whereas data relating to certain behaviors or health conditions may be stigmatizing. The combination of different types of data, both public and app-/research-generated, may further increase its sensitivity.

Fourth, an app's design may or may not provide for return of research results or health-related information. Unregulated research may generate novel individual findings that unregulated researchers may want to return to participants either through the app or by re-identifying app users. This situation raises a variety of issues including the quality and validity of the findings provided, the scientific rigor, validity of data and quality, app users' expectations and understanding of the limitation of these findings and their privacy interests. Return of results is a complicated matter discussed separately in this symposium.[54]

Table 1.

Framework for Categorizing Unregulated Mobile Health Research

		App's primary purpose	
		Research app Data collection for research purpose	**Non-research app** Data collection not for research purpose (e.g., health and fitness app)
Data used by unregulated researcher who is	Original collector / holder of data	Independent research organization develops an app to collect task performance data for a study on Parkinson's disease; self-experimenters develop an app to collect their own biometric data for self-experimentation	For-profit company uses data collected by its pedometer app to study exercise tolerance over time
	Not original collector / holder of data	Patient-led group uses data from a databank, which was collected via a research app and stored for other research uses	Citizen scientist uses data from a melanoma-tracking app to develop an algorithm for detecting potentially malignant moles

E. Quality Issues

Some unregulated health research using mobile devices satisfies even the most exacting methodological standards; other unregulated research raises serious concerns. Quality issues commonly discussed in the literature include poor study design, use of health apps that convey erroneous health information or inaccurately record biometric data, insufficiently rigorous data analysis, and publication of conclusions beyond what the study supports.[55]

The lack of scientific rigor in unregulated health research has significant consequences. A poorly designed study raises ethical issues because even minimal risks are not justified.[56] Flawed research may create serious risks to participants and society, as discussed below.[57] Also, low quality unregulated mobile health research may tend to discredit all similar research.

One methodological area of concern is the selection and utilization of participants for inclusion in unregulated research.[58] Much of the recruitment and conduct of the research takes place on the internet, and such methods have been criticized as placing too great a reliance on self-recruitment and web-based tools that produce inadequately sized or convenience samples.[59] The proportion of highly educated, digitally literate, and well-off people who take part in internet-based research raises concerns about the representativeness of the participants.[60] Self-reporting of symptoms presents other issues,[61] including whether participants have been trained adequately to observe conditions and record health data.[62]

The methodological concerns raised by some types of unregulated health research strongly suggest that humility and setting "modest goals" are important. Such an approach necessitates "an acknowledgement that methodological questions regarding data quality are still in need of addressing and addressing convincingly, as well as an acknowledgement about the limits of what can be expected from public expertise and contributions."[63]

F. Risk of Harms

The lack of legal regulation of certain health research using mobile devices would not be a concern if participants were not placed at risk. Unfortunately, some mobile device and app-based health research poses a significant risk of harm. To date, most of the reported incidents of harm from the use of health apps on mobile devices do not involve research. But, research uses of mobile health apps raise similar issues as health surveillance or wellness uses. Examples include incorrect information and inaccurate measuring, leading to actions or decisions that are adverse to health and wellbeing. The expected increase in unregulated health research using mobile devices strongly suggests that the risk of app-based harms from health research is also likely to grow.[64] Many of the risks described below stem from poor quality in research design, data capture, or analysis. The risk of harm to individuals and groups[65] is mainly in the following four broad categories.

1. Physical and psychological harms can result when apps used in mobile health research provide erroneous health information that participants rely upon to their detriment. These include improperly diagnosing a condition, recommending that the individual forgo essential treatment or medications, or advising the individual to take harmful or ineffective doses of medications or supplements. In one example, the leading app for managing and diagnosing skin cancer correctly classified just 10 of 93 biopsy-proven melanomas.[66] In another example, a systematic assessment of 46 smartphone apps for calculating insulin dose based on planned carbohydrate intake, found that 67% of the apps miscalculated dose recommendations, which put users at risk of poor glucose control or catastrophic overdosing.[67] In 2019, the FDA warned patients and healthcare providers of the risks associated with unapproved or unauthorized devices for diabetes management, including glucose monitoring systems, insulin pumps, and automated insulin dosing systems.[68]

In some cases, harm relates not to the accuracy of the health app, but its use. In one study, some individuals with insomnia who used sleep trackers to improve their sleep became so obsessed with the data produced by the trackers during their sleep that their insomnia worsened, a condition known as orthosomnia.[69] Other tracking apps used by consumers have caused similar harms. For example, orthorexia nervosa is obsessive behavior in pursuit of a healthy diet, which is associated with the use of Instagram, a photo and video-sharing social networking platform.[70] Calorie tracking apps have led to disordered eating caused by self-imposed dietary interventions.[71] Whether a health app is used in a research or a consumer setting, individuals may be harmed if not adequately informed of the psychological as well as physical risks associated with its use.

2. Dignitary harms, including invasion of privacy and harm to one's reputation, can result from insufficient privacy protections that lead to the disclosure or sale of sensitive information.[72] For example, 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 data to Facebook disclosed this fact.[73] 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%).[74]

Mental health data is especially sensitive, and individuals who use mental health apps are likely to be especially vulnerable and perhaps not as attuned to the privacy risks as they ought to be. One app for monitoring people with bipolar disorder and schizophrenia is reported to be "so precise it can track when a patient steps outside for a cigarette break or starts a romantic relationship – and where that new partner lives."[75] Although this app is used in academic research (and presumably regulated), other mental health apps used in other settings are already being

marketed for depression, anxiety, PTSD, and other conditions.[76] These practices raise three concerns: (1) adequacy of disclosure regarding generation and use of the individual's information; (2) adequacy of informed consent that uses click-through agreement to download mental health apps; and (3) the possible invasion of privacy of other individuals identified by geolocation features of the app.

3. Economic harms can result from medical identity theft and other harms caused by inadequate data security or access to an individual's personal information. For example, apps can access a mobile device user's contacts, text messages, photos and videos, credit card information, and facial features,[77] thereby facilitating identity theft. In 2017, there were 1,579 data breach incidents, exposing nearly 158 million Social Security numbers, although it is not known how many of these resulted from health apps.[78] Inadequate security, however, is a well-documented problem with mobile health apps.[79]

4. Societal harms can result in one of two ways. First, socially-identifiable groups or communities may be harmed when questionable research conclusions lead to increased levels of stigmatization or discrimination. Second, improperly designed or performed research can lead to erroneous scientific conclusions that are detrimentally relied upon by numerous individuals – a societal response to the physical and psychological harms mentioned above. Unregulated health research differs widely in its aims, methods, and quality. As with any research, one must assume that some percentage of unregulated health research is poorly designed or performed.[80] Unlike regulated research, however, unregulated research has few checks on scientific rigor, such as an IRB considering whether there is a favorable risk-benefit ratio, grant funders evaluating the scientific merits of a proposal, or a peer reviewed journal evaluating the data analysis.[81] Consequently, erroneous findings of the research can be widely disseminated over the internet

through social networks and other platforms where significant numbers of individuals could learn of and be harmed by a study's scientifically unsound conclusions.[82] Even retracted and repudiated research can thrive on the internet and cause serious harms around the world, as evidenced by the "scientific" articles supporting the anti-vaccination movement [83] and articles advocating harmful self-help measures to treat cancer and autism.[84]

II. Ethical Considerations

A. Introduction

Unlike many other countries, in the United States the laws and regulations pertaining to research with human participants is highly fragmented, which results in notorious gaps in coverage.[85] Whether there is any regulation and, if so, the nature of the regulation depends on the funding source, the identifiability of the specimens and data, and the existence of any applicable state law. Regardless of these differences in legal status and applicable rules, regulated and unregulated research share a common ethical imperative to engage in sound scientific inquiry without undue risk of harm to participants in the conduct of the research and to society in the determination and dissemination of research findings. In Part II, we explore the common ethical foundations of regulated and unregulated health research, and consider them in the context of research using mobile devices and health apps.

This exploration begins by considering the normative grounding for research with mobile devices and health apps. For regulated researchers, their compliance obligations are already prescribed in detail by applicable laws, although the context of mobile devices and health apps presents some novel challenges. Besides legal obligations, many traditional researchers, such as academic medical centers, do not want to violate the trust of their patient communities or the shared

commitment to ethical conduct of their professional staff. For unregulated health researchers, the focus of our study, it may be more difficult to satisfy the following, often-conflicting goals inherent in all health research. The primary goal is to safeguard the autonomy, privacy, and other welfare interests of research participants.[86] A secondary goal is to minimize the burdens on citizen scientists, health app developers, and other unregulated researchers to preserve their flexibility and capacity to innovate. To point the way for achieving these goals we have endeavored to identify essential ethical principles and best practices that should apply to all research, regardless of the current legal regime.[87]

B. Balancing Risks and Benefits

A basic principle of research ethics is that all researchers are ethically obligated to minimize the risks and maximize the potential benefits of research participation.[88] Even though research via a mobile health app typically does not involve invasive testing or medical interventions, it nonetheless exposes participants to risks including physical harms, dignitary and psychological harms, economic harms, and societal harms. Unregulated researchers have the same ethical obligation as other researchers to minimize the above-noted harms to individuals who participate in their research. At a minimum, this means assessing the potential risks to participants in these four areas and identifying strategies to minimize any identified risks. Although specific risks will vary from study to study, minimizing the risks of research via mobile health apps generally means using a rigorous study design, transmitting the least amount of identifiable and/or sensitive data needed to achieve the aims of the study, using stringent criteria for quality when selecting health results or advice that will be provided to participants, and reminding users that health apps are no substitute for appropriate, individualized medical care.

While it is fairly intuitive that the risks of research should be minimized, it is far less clear how investigators are expected to maximize the benefits of research.[89] Interventional research with human participants is based conceptually on the idea of equipoise -- that the research is being conducted because it is truly unknown whether a new intervention or product (like a wearable) truly provides benefits, whether these benefits outweigh its risks, and whether the balance of risks and benefits are superior to some relevant alternative.[90] If these things were already known, then research is unnecessary (and any risks created by the research are ethically unjustified). In most cases, the obligation to maximize the benefits of research simply means that research should be conducted in such a way that participants are not precluded from receiving the benefits of interventions that are already known to work. Consider, for example, an app that is designed to use wearable data to inform a user's workout plan. Even if the developers of the app would eventually want to test whether the app could provide benefits to users in the absence of a personal trainer, they could maximize the benefits to participants by first conducting research with participants who are also receiving the benefits of work with a personal trainer. Only once research of this type had established the benefits and risks of the app in this context would research be conducted to compare the app and a personal trainer head-to-head.

Another threat to an appropriate balance of risks and benefits in unregulated research is the enthusiasm of researchers about the *potential* of the product, like a new wearable or app they are testing. For example, the recruitment materials for a study may make implicit or explicit representations about the benefits of a new wearable when in fact the research is being meant to determine whether the wearable is, in fact, safe and effective. This confusion about equipoise is problematic not only because it may prevent a participant from appropriately considering the risks

and benefits of research participation, but also because research based on the assumption that an intervention or product is beneficial is vulnerable to confirmation bias.[91]

For these reasons, all researchers, including unregulated researchers, should work to suspend their enthusiasm for a new intervention or product when they are conducting research. As much as possible, research should be designed and conducted from a perspective of equipoise. The obligation to maximize the benefits of research should instead be regarded as an obligation to conduct research in the most rigorous way possible so that future users and society as a whole can benefit from the generalized knowledge gained by conducting the research, such as establishing whether a new wearable or app is safe and effective.

Because researchers may be too invested in the success of a study to assess its risks and benefits objectively, it is important for strategies to minimize risks and maximize benefits to undergo review by an individual or entity that is independent from the researcher and is not invested in the outcome of the research. This is discussed in greater detail in section II-F.

C. Consent/Permission

Informed consent has long been considered a cornerstone of research ethics. It is a fundamental demonstration of the ethical principle of respect for persons[92] and, with few exceptions, is required for traditionally regulated research. Federal regulations set forth specific elements of information that must be disclosed to prospective participants, as well as the conditions under which consent is obtained.[93] Even so, informed consent often fails to achieve its goal of adequately informing participants of key study elements. A substantial body of empirical research has documented problems with consent form length and reading complexity.[94] Further, individual-level risk factors, such as low literacy, low educational attainment, and lack of English fluency (for studies conducted primarily in English),[95] may hinder comprehension. Interventions to improve consent

401 comprehension have met with only limited success, although systematic reviews of such studies
402 highlight methodologic challenges.[96]

403 The movement of research into mobile app forms creates at least two new problems. First,
404 as noted elsewhere in this article, mobile platforms can remove many of the regulatory obligations
405 to obtain informed consent by facilitating research outside the traditional institutions to which
406 regulations normally attach. Second, developers and researchers who voluntarily integrate an
407 informed consent process face barriers related to the specific interaction of mobile devices and
408 comprehension.

409 A range of approaches has been suggested for informing app/device users about research
410 use of their data,[97] many of which do not constitute informed consent. For example, "general
411 notification" is an approach involving a brief, broad disclosure that data could be used for research,
412 but offering users no choice in the matter. "Broad permission" similarly involves a brief disclosure
413 but allows users a simple yes/no choice. Although these kinds of models have some advantages
414 (e.g., low burden, efficiency for research), there are significant concerns that they provide too little
415 detail; users are likely simply to click through such disclosures without reading them, and those
416 who do read them may not fully grasp or remember them.[98] Approaches that could meet ethical
417 and regulatory requirements for informed consent include broad consent, categorical or "tiered"
418 consent, and consent for each specific research use. Each of these also entails important
419 advantages and disadvantages from both the user and researcher perspective, many of which have
420 been echoed in other research arenas such as biobanking.[99]

421 Regardless of the approach chosen, key design principles include simple language,[100]
422 integration of visual elements (e.g., photos, drawings), combined with teach-back approaches.[101]
423 Further, experts have suggested including design features that would require some increased

attention or additional action by app users in response to research-related disclosures.[102] Sage Bionetworks has released a series of toolkits[103] and papers[104] related to e-consent, facilitating the implementation of best practices by app developers.[105]

D. Privacy and Security

Privacy and security are fundamental aspects of the ethical conduct of research involving human participants. Adopted by the World Medical Association (WMA) in 1964, the Declaration of Helsinki establishes a duty of physicians involved in medical research to protect "privacy . . . and confidentiality of personal information of research subjects."[106] Consistent with the mandate of the WMA, the Declaration of Helsinki is addressed primarily to physician-researchers, [107] but it also "encourages others who are involved in medical research involving human subjects to adopt these principles."[108]

First prepared by the Council for International Organizations of Medical Sciences in collaboration with the World Health Organization in 1982, the International Ethical Guidelines for Health-Related Research Involving Humans (International Ethical Guidelines) address the use of "data obtained from the online environment and digital tools."[109] In particular, the current (2016) International Ethical Guidelines provide:

> When researchers use the online environment and digital tools to obtain data for health-related research they should use privacy-protective measures to protect individuals from the possibility that their personal information is directly revealed or otherwise inferred when datasets are published, shared, combined or linked. Researchers should assess the privacy risks of their research, mitigate these risks as much as possible and describe the remaining risks in the research protocol. They

should anticipate, control, monitor and review interactions with their data across all stages of the research.[110]

The International Ethical Guidelines also state that researchers should, through an "opt-out procedure," inform persons whose data may be used in the context of research in the online environment of the purpose and context of the intended data uses, the privacy and security measures used to protect such data, and the limitations of the measures used and the privacy risks that may remain despite the implementation of safeguards.[111] If a person objects to the use of his or her data for research purposes, the International Ethical Guidelines would forbid the researcher from using that data.[112]

In addition to the ethical principles set forth in the Declaration of Helsinki and the International Ethical Guidelines, a number of U.S. federal and state laws impose privacy- and security-related obligations on certain research studies or certain classes of researchers. For example, the Common Rule requires IRBs that review and approve research funded by a signatory agency to determine, when appropriate, that "adequate provisions to protect the privacy of subjects and to maintain the confidentiality of data" exist.[113] Similarly, the HIPAA Privacy Rule requires covered entities[114] to adhere to certain use and disclosure requirements,[115] individual rights requirements,[116] and administrative requirements[117] during the conduct of research. Under the HIPAA Privacy Rule, researchers working for covered entities must obtain prior written authorization from each research participant before using or disclosing the participant's protected health information (PHI) unless the use or disclosure falls into one of four research-related exceptions to the authorization requirement.[118] Moreover, the HIPAA Security Rule requires researchers working for covered entities to adhere to certain administrative,[119] physical,[120] and technical[121] safeguards designed to ensure the confidentiality, integrity, and availability of

electronic protected health information (ePHI) and to protect against reasonably anticipated threats or hazards to the security and integrity of ePHI.[122] Finally, the HIPAA Breach Notification Rule requires researchers working for covered entities to provide certain notifications in the event of certain breaches of unsecured PHI.[123]

In light of the ethical and legal principles discussed above, mobile health researchers should implement reasonable privacy and security measures during the conduct of mobile health research. For example, some generally applicable privacy measures include reporting their study results without any individually identifying information, not permitting research results to be used for marketing and other commercial secondary uses without prior explicit consent from each research participant, and not using "click-through" or other non-explicit forms of consent. With regard to security, mobile health researchers should implement reasonable administrative, physical, and technical safeguards designed to protect the security of participant data, such as by safeguarding their physical equipment from unauthorized access, tampering, or theft; and encrypting research data or otherwise making data unintelligible to unauthorized users.

E. Heightened Obligations

The Common Rule recognizes several categories of participants whose vulnerabilities require careful assessment in the research context, including people with diminished capacity to make decisions about participating in research, such as children; those who may lack the autonomy to make decisions due to the institutional context in which the research would take place, such as prisoners or students; and pregnant women for whom decisions would affect both themselves and their fetus.[124] In the context of unregulated mobile health research investigators are not legally bound to follow federal regulations and definitions of vulnerable populations, although many of

the same populations should be regarded as potentially vulnerable to research-related harms, thereby obligating researchers to develop safeguards for their inclusion in health research.

Researchers also have greater ethical responsibilities when health research involves sensitive topics or participants with vulnerabilities that may or may not align with the populations identified in federal research regulations.[125] Specifically, health research using mobile technologies that involves potentially sensitive or stigmatizing information, such as mental, sexual, or reproductive health information, warrants heightened attention to protect individuals' privacy, confidentiality, and security, as noted in the International Ethical Guidelines.[126] Further, mobile technology-mediated research poses a unique challenge in authenticating participants' identities that does not exist when research is conducted face-to-face. Researchers establishing this authentication process must be particularly vigilant when it comes to assessing prospective participants' age and capacity to consent to participate in health research.[127]

Additionally, unregulated health research may create or exacerbate the potential for other harms to individuals and groups. For example, groups that disproportionately rely upon mobile devices for access to the internet, such as those with a low-income, members of racial minorities, and rural residents, may be more vulnerable in the context of mobile health research.[128] Further, people with rare diseases and mental health conditions may be more likely to be identifiable through digital phenotyping, which involves quantification of granular information about individuals using active and passive data collected from mobile and wireless devices.[129] Therefore, app developers and unregulated researchers should carefully assess whether any groups face vulnerability to research-related harms and, if so, ensure that using their information in unregulated mobile health research does not reinforce old forms of discrimination or health disparities, or generate new ones.[130]

F. Independent Ethics Review

Independent oversight of biomedical and behavioral research, widely recognized as an international norm,[131] provides fundamental protection for human research participants. Oversight bodies serve to assess the ethical acceptability of research, evaluate compliance with applicable laws and regulations, and guard against researchers' biases.[132] In the U.S., oversight by an IRB is required for research conducted or funded by the federal government, as well as research under the jurisdiction of the FDA. In general, IRBs are charged with prior review of research involving human subjects to ensure that risks are minimized and are reasonable relative to anticipated benefits, participants are selected equitably, informed consent is sought and documented as appropriate, and there are adequate provisions for monitoring participant safety and for protecting their privacy and the confidentiality of their data.[133]

Researchers whose studies are not subject to these regulations may voluntarily seek IRB review (e.g., from an independent IRB[134]) to obtain ethical oversight as well as meet journal requirements to publish their results. However, researchers choosing to forgo IRB review would not be in violation of legal requirements.

There are several significant reasons why some form of independent oversight would be beneficial for much unregulated research.[135] First, many researchers are unable to objectively and reliably assess and monitor the ethical issues surrounding their own research. Second, whether or not research is technically subject to regulation, the same basic principles and requirements for the ethical conduct of research still apply.[136] Third, given the specific challenges and shortcomings in obtaining effective informed consent in unregulated health environments, protections beyond consent take on even greater importance.

Strong arguments concerning the need for independent oversight notwithstanding, there are reasonable questions about the ability of traditional IRBs to serve in this role for unregulated mobile health research. Criticisms of traditional IRBs highlight time consuming and/or low-quality review processes, excess focus on consent forms, and lack of validated measures of IRB performance leading to unjustifiable variability in IRB procedures and decision-making.[137] Critics also claim that there is little evidence concerning the actual protection provided to participants.[138] Regarding review of studies involving mobile apps and devices, empirical research suggests IRB professionals may be unfamiliar with these novel technologies, uncertain about the risks involved, and unclear on how to become informed—all of which could lead to delays and variability in IRB review.[139]

A range of alternative approaches to independent oversight, both formal and informal, have been proposed. Examples include an oversight board established specifically for unregulated researchers; a forum through which researchers could get feedback and consultation from experts; and ethics training and formal certification for researchers as a replacement for independent oversight.[140] Questions abound concerning any such approach and significant work would be needed to identify and develop effective models that are acceptable to all stakeholders, standardized, sustainable, and can be evaluated. The history of abuses in research with human subjects in the U.S. and around the world has amply demonstrated the limits of relying on researchers to self-regulate as a way to protect participants and their data.

G. Responsible Conduct and Transparency

All researchers, regulated or not, have ethical obligations for responsible conduct of research[141] and transparency.[142] The obligation of all researchers to conduct their research responsibly fundamentally distinguishes scientific from non-scientific inquiry. This mandate includes

appropriate study design, proper data gathering and analysis, and data sharing and publication practices. Other issues under responsible conduct of research include conflicts of interest, author credit on publications, intellectual property, data integrity, and plagiarism.[143]

From the original Declaration of Helsinki in 1964 to the modern open science movement,[144] transparency has been recognized as essential to ensuring the reliability of scientific outputs. However, lack of transparency regarding matters such as research funding and secondary uses of data, seriously erode trust in research. Importantly, the ethical obligation for disclosure of relevant information about health research extends beyond participants (who traditionally receive disclosures in the informed consent process) to the research community and the public. Whereas a lack of transparency to participants goes to the validity of consent, the lack of transparency to the research community and the public goes to the legitimacy of the scientific inquiry and the validity of research findings. The ethics of transparency have been codified by groups ranging from the World Health Organization's Code of Conduct for Responsible Research[145] to the grassroots cybersecurity research movement, I Am the Cavalry's Hippocratic Oath for Connected Medical Devices.[146]

There are several unique barriers faced by unregulated health researchers as they attempt to uphold their ethical obligations for responsible conduct and transparency. First is the "black box" problem. It can be difficult even for experienced researchers to understand the engineering that underlies mobile health tools. Which data are collected, how they are stored, and with whom they are shared may be obscurely presented, if at all. When developing mobile health devices, researchers may not realize the "hackability" of their devices,[147] thereby permitting the unethical exploitation of their devices. In addition, mobile health data may collect far more information than

needed to accomplish the researcher's goals; for example, recording an individual's exact GPS coordinates when a less precise displacement vector would do.

H. Proposed Ethical Frameworks

Beyond the ethical principles discussed above, a range of other principles have been proposed to guide the use of digital health data in unregulated research. These include, but are not limited to, recommendations that digital health information be accurate;[148] that experts (in experimental design, data analysis, research ethics) be accessible;[149] and that the most appropriate ethical frameworks/governance structures for any given project will vary depending on the characteristics of the researchers, participants, and research design.[150]

Differences between traditional research and citizen/community/patient-directed studies have led some to question whether the traditional paradigm of ethical review (e.g., IRB/REC involvement) is appropriate in participant-led initiatives.[151] Some have argued that IRB/REC involvement may "promote decisions specific to data ownership, data management, and informed consent that directly conflict with the aims of research that is explicitly participant-led."[152] In response, several more fluid and adaptable approaches have been put forth.

Some scholars[153] have proposed a citizen science governance framework that exists along a continuum in which "people-related" choices (e.g., regarding project membership and privacy of members personal data) and "information-related" decisions (e.g., privacy of, access to, and ownership of data) are made using a more rigid top-down approach (e.g., platform developer) or more flexible, bottom-up (e.g., project managers) approach depending on the specific needs and goals of the project. In determining the most appropriate framework, some commentators recommend that studies make explicit the "full spectrum of meanings of 'citizen science,' the

contexts in which it is used, and its demands with respect to participation, engagement, and governance."[154]

Other experts suggest that the specific ethics/governance expectations and obligations be, in part, determined by the researcher context; specifically, whether unregulated researchers are operating within state-recognized or state-supported institutions and/or are engaged in profit-making.[155] When research occurs within such institutions or for-profit, then standard ethics review (identical obligations of oversight) would be appropriate.[156] A risk-based approach can be used to divide all other types of projects (non-institutional and non-profit) into two categories. Studies in which the research involves more than minimal risk should require some form of ethics review, possibly equivalent to expedited review, or through open protocol crowd-sourcing ethics review. Studies involving no more than minimal risk would not require formal ethics review, but would still require oversight with respect to basic ethical principles and legal requirements.[157] A range of ethical approaches also may be gleaned from international sources.[158] After reviewing these many sources of ethical frameworks, we have used fundamental ethical and policy considerations to guide our recommendations.

III. Ethical Issues and Policy Recommendations

A. Introduction

The opinions of policymakers, stakeholders, academics, and others on unregulated health research diverge widely. On the one hand, some experts advocate extending the Common Rule to all researchers, arguing that regardless of the funding source all research participants should be entitled to the same protections, such as a balancing of risks and benefits, informed consent, and confidentiality. Some of these experts take an all-or-nothing approach. If political considerations

make it impossible to obtain comprehensive coverage under the Common Rule, they reject the idea of accepting lesser protections, such as voluntary ethics consultation for researchers and optional external ethics review, because they believe it erroneously assumes that partial protections are sufficient. Some view these measures as a "watered-down version of the Common Rule."

On the other hand, many unregulated researchers and their advocates strongly object to *any* regulation or governmental involvement in unregulated health research, including mobile device-enabled research.[159] They view regulation of this research as unnecessary and burdensome governmental meddling into valuable scientific inquiry. Some even oppose optional government consultation or educational assistance to unregulated researchers on the grounds that it is the first step to regulation.

After careful consideration, we decline to endorse either of these positions toward unregulated research. In the sections that follow, we make the case for a middle ground approach based on pragmatism. We recognize that such a position requires a deft balancing of all interests and that our position is susceptible to criticism from both sides of the issue. To address both sides, we begin with the argument that there is no need to have any new efforts directed at unregulated health research, including research using mobile devices and health apps.

In our view, the current laissez faire approach to unregulated health research in the U.S. is not in the best interests of participants, researchers, or the public. We begin by noting that most other countries regulate all biomedical research regardless of the funding source, [160] and therefore the U.S. is an international outlier in this regard. Nevertheless, recent experience with the Common Rule amendment process (discussed in the following section) makes it highly unlikely that in the foreseeable future Congress will extend the Common Rule to all research. There might be some expansion of state research laws, but the likelihood and desirability of state legislation

and enforcement in this area is unclear. In the current political atmosphere, we believe that sensible, reasonable, and demonstrably effective measures, though inferior to comprehensive coverage of the Common Rule, are still far superior to doing nothing. It also could be asserted that many of our recommendations to assist unregulated researchers should be available to regulated researchers as well. We do not quarrel with that view; we merely note that our task is to address unregulated research using mobile devices and not to address all of health research.[161]

We similarly reject the position of many unregulated researchers that an increased emphasis on research safeguards and ethical conduct is unnecessary. Although unregulated research using mobile devices rarely involves invasive or high-risk procedures, it still may cause a variety of harms.[162] At a time when unregulated research is expanding, it is necessary and appropriate to consider a wide range of measures to protect the interests of research participants and the public. No researchers, regardless of their funding, training, or motivation should engage in conduct that creates unreasonable risks to research participants, and oversight is a key way of ensuring ethical grounding of all research with human participants.[163]

Our recommendations utilize a combination of methods, including education, consultation, transparency, self-governance, and regulation. We support a risk-based approach to research ethics oversight whereby all no-risk or minimal-risk research would be exempt or subject to expedited ethics review. This principle, as applied to unregulated research, means that the level of risk would determine the degree to which traditional research ethics requirements apply.[164] We believe that in the absence of expanded coverage of the federal research regulations the measures that follow will help protect participants in unregulated health research using mobile devices while still facilitating innovative methods of scientific discovery.

B. Federal Research Regulations

The National Research Act[165] was enacted in 1974 in the aftermath of public disclosures and congressional hearings documenting the outrageous and unethical research practices involved in the Tuskegee Syphilis Study.[166] The Department of Health, Education, and Welfare (HEW) first published regulations for the protection of human subjects in 1974.[167] The Department of Health and Human Services (HHS), the successor to HEW, led an inter-agency process that culminated in 1991 with publication of regulations for research conducted or funded by signatory federal departments and agencies.[168] Because of their broad applicability, the Federal Policy for the Protection of Human Subjects became known as the "Common Rule." The jurisdictional basis of the Common Rule was the federal government's conduct or funding of the research. Separate regulations were promulgated by the Food and Drug Administration (FDA) in 1981, applicable to research conducted in anticipation of a submission to the FDA for approval of a drug or medical device.[169]

When it was originally adopted in 1991, the Common Rule's coverage of federally-funded researchers was generally considered sufficiently comprehensive because the predominant model of research, especially biomedical research, involved centralized research at large institutions. These recipients of federal funding also generally agreed to abide by the Common Rule in all research conducted at their institutions, regardless of the funding source.[170] The Institute of Medicine,[171] the National Bioethics Advisory Commission,[172] and other expert bodies have proposed that the federal research regulations should apply to all human subject research regardless of the funding source. The recent growth in unregulated research described in this article has added another dimension to this ongoing policy debate.

The lengthy and contentious rulemaking culminating with the recent revisions to the Common Rule,[173] published in 2017 and effective in 2019,[174] illustrates the difficulty in expanding

the scope of the federal research regulations. In 2011, HHS, in coordination with the White House Office of Science and Technology Policy, published an Advanced Notice of Proposed Rulemaking, requesting public comments on how the existing federal research regulations might be modernized and improved.[175] One specific area in which comment was sought was extending the Common Rule to all studies, regardless of the source of funding. In 2015, the Common Rule agencies issued a Notice of Proposed Rulemaking,[176] which limited the proposed expansion of the Common Rule to all clinical trials or alternatively those clinical trials presenting greater than minimal risk, regardless of the funding.[177] By 2017, the final rule issued by the Common Rule departments and agencies abandoned altogether the proposal to expand the coverage of the Common Rule.[178]

In light of this recent experience and the lack of political and public support for such a fundamental change, we have chosen not to focus our recommendations on expanding the coverage of the Common Rule to include all biomedical research regardless of the funding source.[179]

C. State Research, Data Protection, and Genetic Testing Laws

1. State Research Laws

Recent state legislative activity in the areas of research regulation and consumer protection[180] indicates a greater willingness of states to become involved with these issues, in part because of inaction by Congress. Because mobile research applications can collect data from participants who reside in different states, uniformity of laws (and uniformity of interpretation of such laws) is critical for implementation and compliance. Therefore, if state regulation is viewed as the best way to obtain comprehensive regulation of health research, the adoption of a model or uniform

state law is preferable to wildly varying state enactments. Of the state research laws enacted thus far, we believe the Maryland law is the best.

a. Maryland

In 2002, Maryland enacted its state research law for "the purpose of requiring a person conducting human subject research to comply with federal regulations on the protection of human subjects."[181] Accordingly, Maryland regulates "all research using a human subject," regardless of whether such research is federally funded,[182] and prohibits "a person" from "conduct[ing] research using a human subject unless the person conducts the research in accordance with the federal regulations on the protection of human subjects (the Common Rule)."[183]

One reason the Maryland law is desirable in the context of mobile device-mediated health research is its unrestricted use of the word "person." The Maryland law applies to all researchers, including traditional scientists, independent scientists, citizen scientists, and patient researchers, as well as any other person who conducts research.[184] Other state research laws discussed below apply to a narrower class of researchers, such as researchers who are licensed physicians or researchers who conduct research in a licensed health care facility.

A second desirable feature of Maryland law is its definition of "federal regulations on the protection of human subjects." The definition specifically references "Title 45, Part 46 of the Code of Federal Regulations [the Common Rule], *and any subsequent revision of those regulations*."[185] The Maryland law anticipates the possible revision of the Common Rule and expresses a clear desire for Maryland research to be conducted in accordance with the most current version of the Common Rule.

If the Maryland law were used as a model for other states it would promote uniform requirements and protections with both the federal Common Rule and state research laws. As with

all issues of federalism, however, the downside of uniformity and preventing a patchwork of state laws is that it prevents other states from adopting innovative approaches. Pioneering research laws implemented in state "laboratories of democracy"[186] might identify improved ways to address emerging issues, such as health research with mobile devices.

b. Other State Research Laws

Six other states, Virginia, New York, California, Illinois, Wisconsin, and Florida, also have enacted research laws. None of these laws address the unique features of mobile device-mediated research. They also are not comprehensive or provide weaker protections for research participants than the Common Rule.

Of these other state laws, Virginia provides the most comprehensive coverage for non-federally funded human research,[187] including detailed requirements for the formation of human research review committees,[188] criteria for review committee approval of research,[189] and mandatory provisions for informed-consent-to-research statements.[190] Compliance with unique state laws would prove difficult for mobile device-mediated health researchers who collect data from study participants residing in various states.

The New York research law establishes a policy of protecting state residents against "pain, suffering or injury resulting from human research conducted without their knowledge or consent."[191] However, the New York law narrowly defines "human research" as investigations involving physical or psychological interventions.[192] The New York law would thus leave unprotected participants of mobile device-mediated, solely information-gathering research studies.

The California Protection of Human Subjects in Medical Experimentation Act[193] establishes a detailed "bill of rights"[194] and a series of explicit informed consent requirements[195] designed to benefit subjects of medical experiments,[196] as well as damages for research conducted

without consent.[197] The law, however, only applies to "medical experiments" and would not protect participants of mobile device-mediated informational research studies.

The Illinois Act Concerning Certain Rights of Medical Patients applies only to physician-researchers who conduct research programs[198] involving hospital inpatients or outpatients and therefore would not apply to most participants in health research using mobile devices because they are not hospital inpatients or outpatients.

The Wisconsin Patients' Rights law[199] only protects "patients," defined as certain individuals with mental illness, developmental disabilities, alcoholism, or drug dependency who receive treatment for such conditions in certain licensed health care facilities.[200]

Finally, Florida's Patient's Bill of Rights and Responsibilities Act, [201] only applies to patients of licensed health care providers and health care facilities.[202]

2. State Data Protection Laws

In addition to state research laws, many states have data breach, data security, and data privacy laws that are potentially applicable to mobile device-mediated research.[203] In particular, all fifty states and the District of Columbia have enacted data breach notification laws that require the notification of data subjects of certain informational breaches in certain contexts.[204] In addition, thirty-six jurisdictions have enacted statutes designed to protect the security of certain data sets, and fifteen jurisdictions have enacted statutes designed to protect the privacy of certain data sets.[205] In some states, these statutes already apply to mobile device-mediated researchers who conduct informational health research.[206] In other states, minor amendments to the definitions of "covered entity," "personal information," and "doing business in the state" would be necessary before the statutes would apply to mobile device-mediated health research.[207]

A concern about both state research and data protection laws is that unregulated researchers are unlikely to know that such laws even exist, and therefore public education programs should be part of any legislative strategies.

3. State Genetic Testing Laws

Many states have laws regulating genetic testing that may be relevant to unregulated health research using mobile devices, even if the testing is performed by a DTC genetic testing company or other entity unaffiliated with the researchers. Among the most common types of provisions are those requiring informed consent,[208] establishing the privacy and confidentiality of genetic information,[209] and prescribing certain retention or disclosure practices.[210]

Recommendations for the States

1-1. States that do not currently regulate all non-federally funded research should consider enacting a comprehensive law (or amending existing laws) to regulate all research conducted in the state.

1-2. States considering such legislation should review the Maryland research law, which contains a broad definition of "person" performing research and expressly applies the most recent version of the Common Rule.

1-3. States also should consider extending the application of data breach, data security, and data privacy statutes to all mobile device-mediated research.

1-4. States also should consider extending the application of genetic testing laws to all research conducted in the state.

D. National Institutes of Health

The National Institutes of Health (NIH) is the world's largest public funder of biomedical research, with a 2019 research budget of $39.2 billion.[211] More than 80% of the research budget funds extramural research.[212] Beyond its size and budget, there are additional reasons why NIH would be a logical entity to play a leading role in health research conducted by unregulated researchers using mobile devices. First, NIH currently has numerous programs promoting the development of novel and emerging research strategies, such as its Common Fund initiatives.[213] Second, NIH has a variety of programs for scientific education and workforce development, including science education resources for students and educators[214] and its specialized information services designed to provide access to quality and accurate health information in underserved and special populations.[215] Third, NIH already has demonstrated an interest in mobile health[216] and citizen science[217] through ongoing programs, and as evidenced by funding this grant through the National Cancer Institute, National Human Genome Research Institute, Office of Science Policy and Office of Behavioral and Social Sciences Research in the Office of the Director.[218]

There are three main reasons why some individuals and groups might not view NIH as an appropriate entity to play a leading role in this area of research. First, NIH may be regarded as epitomizing the traditional research establishment to which many citizen scientists, DIY researchers, self-experimenters, and other unregulated researchers object. Second, NIH maintains a detailed system of compliance and oversight for its extensive grant portfolio, and the prospect of NIH – even symbolically -- knocking on the door of every basement and garage laboratory would be most unwelcome. Third, NIH is not a source that independent health app developers would likely consult to obtain source data and guidance on developing apps used for health research.

We believe these concerns can be addressed. We envision that the role of NIH would be limited to serving as an information clearinghouse, supporter of research infrastructure

development, and convener working with a range of governmental and nongovernmental groups and individuals. NIH would not have any regulatory role nor would it be involved in the direct funding of unregulated research. NIH would maintain a low profile and a light touch in promoting quality in unregulated health research and in safeguarding the welfare of research participants. This limited role for NIH is in keeping with its extant legal authority. Although the goals for the conduct of regulated and unregulated research are aligned, alternative procedures are necessitated by the current legal provisions. It remains to be seen how effective alternative means would be when applied to unregulated researchers; nevertheless, measures adopted to aid unregulated researchers (e.g., training programs) could serve as a way to assess the efficacy of similar measures for regulated researchers.

The recommendations that follow propose that NIH expand its efforts to assist unregulated researchers, research participants, and health app developers. NIH's first priority in this area should be to serve as a repository of information essential to all stakeholders in unregulated health research. We recommend that an advisory board of diverse stakeholders (e.g., citizen scientists, DIY researchers, patient-directed researchers, app developers) be appointed to assist NIH in its activities, thereby providing practical information and enhancing the credibility of NIH's efforts. NIH should fund studies on unregulated health research to determine the most effective ways of encouraging voluntary adoption of best practices and developing open-source tools. In consultation with the Office for Human Research Protections (OHRP), NIH should work to create and disseminate educational tools about research protections. In consultation with OHRP, and with input from grantees, NIH should also study the feasibility of supporting cost-free, independent, external research review organizations to advise unregulated health researchers how to ensure that all their research is consistent with essential ethical principles. An alternative model

with less direct involvement of NIH is for grantees to take the lead in information sharing, education programs, and consultation services for unregulated researchers.[219]

Finally, surveillance is a cornerstone of public health efforts to assess trends over time and then evaluate the impact of interventions.[220] This concept, however, has not yet been applied to mobile health research because there is no specific reporting of mobile health research and no required adverse event reporting for unregulated researchers. Therefore, a surveillance program should be established to estimate the amount of mobile health research, including unregulated health research over time as even those basic figures are not known. Surveillance also would include assessing and categorizing adverse events using rigorous standards for case definitions. Over time, these data can be used to improve how mobile research applications are developed and used in research, with the ultimate goal of reducing adverse events.

Recommendations for the National Institutes of Health (NIH)

2-1. NIH should expand its support for unregulated health researchers and centralize responsibility for providing assistance. NIH may accomplish this by establishing a new Office of Unregulated Health Research, designating an existing Institute or Center to oversee initiatives on unregulated health research, funding grantees to provide assistance to unregulated researchers, or through other means.

2-2. NIH should appoint an advisory board of diverse stakeholders to assist the NIH official or entity in charge of unregulated health research.

2-3. Unregulated health researchers need accessible, consolidated, updated, and curated information about research laws and ethical considerations from a trusted source. NIH should provide technical and understandable information about mobile and wireless

technologies for app developers, researchers, and research participants. Therefore, NIH should develop and maintain a website containing the following.

a. Information and FAQs identifying the laws applicable or inapplicable to health research, including the Common Rule, FDA, FTC, state research laws, and the HIPAA Privacy Rule;

b. Information about externally developed best practices and ethical principles for unregulated health research;

c. Directory of open source tools for health research apps, including sample consent documents, privacy protection measures, and security information; and

d. Directory of resources for technical assistance.

2-4. NIH should fund studies on unregulated mobile health research to determine the most effective ways of encouraging compliance with best practices, attaining and maintaining quality, and developing open-source tools.

2-5. NIH should, in consultation with the OHRP, work with citizen science groups and other organizations of unregulated researchers to support educational programs for mobile health app developers, unregulated researchers, and participants, as well as to provide technical support.

2-6. NIH, in consultation with OHRP, should consider the feasibility of establishing or supporting cost-free, independent, research review organizations to advise unregulated researchers on identifying and resolving ethical challenges raised by their research.

2-7. NIH, in consultation with OHRP, the National Science Foundation (NSF), and other public and private entities should support the establishment of a surveillance system to monitor, categorize, and track the rate of health research using mobile devices. The

surveillance system also should capture the incidence and nature of adverse events caused by health research using mobile devices in both regulated and unregulated research.

E. Food and Drug Administration (FDA)

The Food and Drug Administration (FDA) has jurisdiction over research with human participants in two main ways. First, clinical research conducted in contemplation of a submission to the FDA for approval of a drug or medical device is subject to detailed regulations similar to the Common Rule.[221] Among other things, the regulations require informed consent,[222] review by an IRB,[223] and disclosure of investigators' financial conflicts of interest.[224] Second, the FDA has jurisdiction over medical devices that may be used in research, which potentially creates a pathway for the FDA to regulate research with human participants conducted by unregulated researchers. This section and the recommendations that follow are concerned with this second aspect of FDA jurisdiction.

The Food, Drug, and Cosmetic Act (FDCA), as amended,[225] provides the FDA with a broad public health mandate that includes regulation of medical devices. Congress defines devices that are subject to FDA regulation as including any "instrument, apparatus, implement, machine, contrivance..." that is "[i]ntended for use in the diagnosis of disease or other conditions, or in the cure, mitigation, treatment, or prevention of disease, in man or other animals" and components and accessories of such devices also are regulable as devices.[226] Mobile health apps potentially fall within the scope of this definition. In recent years, this created concerns that the cost and burdens of FDA oversight might chill innovation in mobile medical applications and wellness products that could benefit consumers.[227]

To allay these concerns, the FDA issued guidance documents in 2013 and 2015 indicating its intent to regulate mobile apps only if they performed medical device functions that could pose a risk to patient safety if the mobile app failed to function as intended.[228] In 2016, the 21st Century Cures Act[229] formalized this policy by amending the FDCA's definition of a device to remove five categories of software from FDA's jurisdiction.[230] One of the exclusions relates to software for encouraging wellness or a healthy lifestyle, provided the software does not cross the line into "diagnosis, cure, mitigation, prevention, or treatment of a disease or condition."[231] This category, often referred to as general wellness software, includes such things as fitness trackers and medical calculators (e.g., for body mass index).

In 2019, the FDA issued final guidance that further clarifies the line between regulated and unregulated wellness software after 21st Century Cures.[232] This is part of a larger, ongoing effort that the agency launched several years ago to implement a Digital Health Innovation Action Plan and create a Center of Excellence in Digital Health to improve its oversight of software.[233] FDA embraces a risk-based framework for regulating health information technology in concert with the Federal Communications Commission (FCC) and the Office of the National Coordinator for Health Information Technology (ONC), as directed by the Food and Drug Administration Safety and Innovation Act (FDASIA) of 2012,[234] with the aim of limiting regulatory duplication or overstepping.[235] Additionally, ONC, FDA, FTC, and the HHS Office for Civil Rights (OCR) have published an online, interactive decision tree to aid app developers in correctly identifying the federal laws that apply to their apps.[236]

We endorse the FDA's focus on clarity and efficiency in digital health regulation, but there are unresolved issues relating to research that uses mobile health apps when—as often will be the case—such research is not regulated by the Common Rule. There is a risk that such research might

encourage participants to use low-risk general wellness devices in new ways for which the devices are not safe and effective. This potential for repurposing and misuse exists because of the way FDA determines whether a device is a low-risk general wellness device that is exempt from FDA oversight versus a medical device subject to FDA regulation. This determination does not necessarily reflect intrinsic properties of the device itself, in terms of the health characteristics that it is capable of measuring or the quality of the data it produces. General wellness devices sometimes produce data that closely resemble data from an FDA-regulated medical grade device.

For regulatory purposes, the distinction between a general wellness device and a medical device turns on the device's intended use.[237] FDA's algorithm for assessing the intended use of a device is set out in the agency's regulation at 21 C.F.R. § 801.4. As a general matter, a device's intended use refers to the objective intent of the "the persons legally responsible for the labeling"[238] of the device, which in most instances is the device's manufacturer. Section 804.1 allows FDA to consider direct and/or circumstantial evidence of the manufacturer's intent. Direct evidence would include claims the manufacturer or its representatives made about the device, such as in its labeling, advertising matter, and oral and written statements about the device.[239] The allowed circumstantial evidence includes facts showing that the manufacturer knew that the device was being misused for purposes other than those for which it was labeled and advertised.[240]

In practice, however, it is unlikely that the FDA would hold a manufacturer responsible for other people's misuse of its device, even if the manufacturer was aware of the misuse. As a leading treatise observes, "FDA has rarely attempted to classify a product as a drug or device in the absence of relevant representations by the manufacturer or distributor."[241] In other words, the agency generally bases its decisions on the direct evidence: statements the manufacturer made in labeling, advertising, and marketing of the device. The FDA has never disclaimed its authority to establish

a product's intended use based on circumstantial evidence of a known misuse, but it is rare for FDA to assert that authority,[242] and even rarer for FDA to prevail in court when it does.[243] The recent FDA guidance on general wellness devices treats manufacturers' claims about a device as the main source of evidence the agency will use to distinguish (unregulated) general wellness devices from (regulated) medical devices.[244]

A device that is lawfully on the market, but which is being used in research in a novel way that goes beyond its intended uses, potentially becomes an investigational device that requires an investigational device exemption (IDE).[245] The IDE regulations aim to protect study participants when they are exposed to risk from devices being used in ways that FDA has not established are safe and effective, and to ensure that the devices produce valid data. The IDE regulations apply to research sponsored by device manufacturers trying to generate data for submission as part of an FDA premarket review, but the agency emphasizes that its IDE requirements also may apply in other research settings. There are many unresolved questions about whether and how these regulations would apply to unregulated health research using mobile devices.

The FDA gains its authority to regulate research as an incident of its authority to regulate medical products such as drugs and devices. This implies that FDA's research regulatory mandate is narrower in scope than the Common Rule. Part 812 allows FDA to regulate studies *of* devices ("clinical investigations of devices to determine safety and effectiveness")[246] but not studies that merely use devices as tools to explore basic scientific or medical questions. The agency's own training materials state that no IDE is required for "basic physiological research" that is "investigating a physiological principle" with "no intent to develop the device for marketing," if the investigation is "only using the device to address the research question."[247]

Although FDA generally does not regulate "investigations to expand medical knowledge or conduct fundamental research,"[248] there are a few exceptions that allow FDA to regulate such research. One exception is for broad scientific studies that incorporate a device study. "If the expansion of medical knowledge or the conduct of fundamental research involves an investigation to determine the safety or effectiveness of a device, an IDE will be required."[249] A second exception allows FDA to require an IDE if a broad scientific study uses a device in novel ways that pose "significant risk" for the research subjects.[250] In some contexts, FDA has taken the position that research poses significant risk if patient-specific results are returned to participants. FDA has not clarified how these principles apply to citizen science projects. Such studies often are observational rather than interventional in nature, so the risk they pose may be minimal. Moreover, it is hard to characterize research as "returning" patient-specific results to participants, when the participants collected the data and had possession of it in the first place.

Another regulatory risk involves unlawful promotion of unapproved uses of legally marketed devices.[251] The IDE regulations prevent research sponsors, investigators, and persons acting on their behalf from communications that promote an investigational device that has not been cleared or approved[252] or that represent the device as safe and effective for the purposes for which it is being studied.[253] There is a risk that FDA might deem a citizen science project to be promoting unapproved uses of general wellness devices. This could chill constitutionally protected scientific speech unless the boundaries of FDA's efforts to regulate such "promotion" are carefully drawn.

Many citizen science and other nontraditional research projects are "sponsor-investigator" studies in which the sponsor and the investigator are the same person. Sponsor-investigator studies are believed to pose special risks for human research participants, because they lack the inherent

checks and balances of having a separate sponsor and investigator keeping an eye on one another's activities. In 2005, an FDA official noted a high incidence of participant protection problems in such studies.[254] Some of FDA's training materials suggest that FDA can require an IDE for sponsor-investigator studies, regardless of whether the study sponsor aims to submit data to FDA, to develop a new device for marketing, or to expand the intended uses of a legally marketed device."[255] This position has been questioned,[256] but the agency has not reversed it, and it adds to the regulatory uncertainty around citizen science projects.

Recommendations for the Food and Drug Administration (FDA)

3-1. The FDA should continue its interagency collaborative efforts to reduce regulatory duplication and identify and assess areas unaddressed by current regulations. One area for immediate interagency consideration is how best to ensure transparency in validation of mobile health app algorithms, in situations where FDA has jurisdiction to regulate such devices.

3-2. The FDA should increase its engagement with the health app developer community to raise awareness of its guidance documents, including those issued in September 2019.

3-3. The FDA should require developers of mobile health apps subject to its jurisdiction to make transparent disclosures regarding the intended use (including research) and technical capacities of their apps, especially mobile medical apps.

3-4. The FDA's guidance documents have failed to address how its regulations apply to citizen-led research using data from mobile health apps. In particular, the FDA needs to clarify the following: (1) when such research may require an IDE; (2) what forms of research using data from mobile health apps constitute "significant risk" research under the IDE regulations; (3) how the concept of a "sponsor-investigator study" applies to nontraditional

and citizen-led research; (4) what forms of communication about citizen science projects could subject organizers to charges of unlawful promotion of unapproved uses of a device; and (5) what constitutional constraints limit the FDA's power to regulate nontraditional, citizen-led research efforts.

F. Federal Consumer Protections through the FTC and CPSC

Federal agencies tasked with ensuring consumer protection with regard to commercial products and services, such as the Federal Trade Commission (FTC) and the Consumer Product Safety Commission (CPSC), are well-positioned to regulate mobile platform-based health research because they can take more comprehensive approaches to regulation.[257] As mentioned above, the FDA's jurisdiction does not extend to some mobile health apps' software functions and uses, such as fitness trackers and medical calculators, and therefore regulatory responsibility could fall to consumer protection agencies.

The FTC is responsible for preventing unfair competition and unfair or deceptive acts or practices by entities engaged in or affecting commerce. It can seek monetary redress for consumer injuries, make legislative recommendations, and prepare reports. The FTC's preventative mission positions it to use self-regulation enforcement mechanisms; this means that the FTC does not need to wait until consumers are harmed before it can act. By using selective enforcement within an industry the FTC can protect mobile technology-mediated health research participants, including their health privacy, through regulation of unfair trade practices.[258]

The FTC could be particularly useful in regulating the adequacy of consumer technology companies' and app developers' privacy policies and practices, transparency, and fairness practices in the research they undertake or facilitate. The FTC has taken enforcement actions against flagrant offenders of consumer protection in the health space since 2011, with a particular

focus on commercial entities that have claimed to identify or cure health conditions such as acne, skin cancer, and vision problems.[259] Its enforcement actions have focused on truth-in-advertising, substantiation requirements to support product claims, and privacy and security breaches and insufficiencies.[260] Further, the FTC co-produced a web-based interactive tool with HHS, ONC, OCR, and FDA, housed on the FTC website, to guide app developers about the federal laws that apply to the development and implementation of mobile health apps.[261] These efforts indicate that the FTC is familiar with and monitoring mobile health, which could include mobile health research, for instance in surveilling the fairness of algorithms used and generated in unregulated mobile health research.

The CPSC is a federal agency authorized to protect consumers through surveillance functions and enforcement. In the digital arena, the CPSC issued a report to guide consumer safety and protection in relation to digitally connected devices entitled "A Framework for Safety for the Internet of Things."[262] In this framework the CPSC focuses on the potential for these devices to result in physical harms, illness, and death of consumers. Although narrow in scope, this framework illustrates that the CPSC sees the Internet of Things, within which mobile-platform enabled health research is a component, as within its jurisdiction. Furthermore, recognition that digital connectivity can result in psychological, emotional, and social harms that can be deeply injurious suggests that unregulated mobile health research could be subject to CPSC's regulation.

The CPSC's jurisdiction may extend to circumstances and conditions not covered by the FDA, but the CPSC has limited regulatory tools. Thus, unless its regulations and enforcement powers are strengthened, merely having jurisdiction does not necessarily translate into the ability to exercise meaningful regulatory oversight.

Recommendations for the Federal Trade Commission (FTC) and the Consumer Product Safety Commission (CPSC)

4-1. The FTC should increase its efforts to encourage self-regulation of unregulated mobile health researchers by providing guidance and educational resources to app developers, unregulated researchers, and participants in unregulated mobile health research through, among other things, best practice guidelines and web-based, interactive educational tools.

4-2. The FTC should promote privacy, transparency, and fairness in unregulated mobile health research using preventative and remedial approaches, such as the following.

a. The FTC should increase targeted enforcement actions against developers of unregulated mobile health research platforms who engage in deceptive or unfair trade practices (e.g., making false or misleading statements, failing to provide adequate privacy or security for mobile Internet-connected devices) and seek monetary redress and other appropriate relief on behalf of injured consumers.

b. The FTC should develop and provide multi-media educational materials for consumers about the kinds of harms and complaints being monitored, and publicize bad actors in the unregulated mobile health research sector through consumer advisories.

4-3. The CPSC should increase surveillance and monitoring of research software, applications, and systems enabled through mobile, internet-connected devices by establishing a consumer hotline or website for reporting safety concerns, such as data breaches, and it should assess monetary penalties against researchers and developers who violate consumer product safety regulations pertaining to internet-connected mobile devices.

G. Consumer Technology Companies and App Developers

Consumer technology companies fall along a spectrum of size and power, but taken together represent the dominant players in unregulated mobile health data collection. These companies are familiar with regulation through their interactions with Congress, the FCC, FTC, and other government agencies, but the health policy issues represent a relatively novel space for most companies.

Consumer technology companies may be divided into two categories -- platforms and startups -- each of which has two sub-categories. We break down platforms into app stores and handset manufacturers, and startups into those making research apps and wearables. This division recognizes that companies that have achieved market dominance have significantly more economic power to create actual change than early stage startups, as well as more exposure to regulation via traditional channels over time. Startups also have radically different resource levels and incentives compared to platforms. In this division, we also note that the primary regulators of startups may well be the platforms that broker access to customers for the startup.

Apple is perhaps the clearest example of a consumer platform as regulator, recently acting to protect consumer privacy with a unilateral technical change around email login.[263] Within our topic area, Apple already encodes visual informed consent (i.e. an interface that requires app users to slow down and reflect on key issues through the use of icons, videos, and other methods)[264] into ResearchKit developer documentation and requires ResearchKit apps to have IRB approval regardless of whether the Common Rule applies.[265]

A wide variety of consumer technology platforms exist. Microsoft's Windows is a platform, as is Amazon. For our purposes, we will focus on a very small subset of consumer technology companies that are most relevant to unregulated mobile health research: app stores as platforms, phone+wearables and their related mobile applications as platforms (i.e., from Apple

or Google), research apps from startups, and "wearable" devices from startups. This focus excludes certain cases, but allows us to look at the vast majority of interactions with technology companies driving mobile research.

Platforms at their most basic are "digital infrastructures that enable two or more groups to interact."[266] The race to create a platform that enables many groups to interact defines much of the contemporary consumer technology space; massive amounts of capital pour into platforms to claim the network effect through subsidized products.[267] The vast majority of consumer technology companies involved in unregulated health research aspire to platform status. Thus, for our purposes, what distinguishes a platform from a startup is simply the question of market adoption. Has the company achieved enough power to serve a soft-power regulatory function, or is the company likely to make choices in hopes of achieving that power while being regulated in turn by larger platforms? This type of ontology is necessary to delineate apps that are truly about self-tracking or "n of we" such as those seen in quantified self[268] – primarily observational, with little aspiration to scale to thousands or millions or billions of users – from those funded by venture capital aspiring to monetize research data.

The app store duopoly puts Apple and Google in a de facto regulatory position, a situation that is not likely to change in the near future. Their differing review regimes represent forms of governance[269] that, for example, lead to a difference in the ability of developers to implement spyware or to submit "copycat" applications[270] ranging from innocuous clones to apps that actively install malware and spyware. Android users are also shown to be vulnerable to "grayware" -- "potentially harmful apps" falling somewhere between utility and exploitation, typically just outside the illegal space.[271] Our policy recommendations for these two companies therefore leverage this "soft power" to regulate the vast world of applications used in mobile health research.

Hardware manufacturers is a broad category. It includes phone handsets, although phones are often quite secure hardware platforms compared with other types of devices, such as the booming and varied field of "wearable health trackers." Hardware companies must balance consumer-facing priorities and ease of pairing with an app on a mobile device with security features. New features that would significantly improve privacy and security – for example, encryption of all data "at rest" (on the device itself) typically drains battery performance,[272] and thus is often left off devices during the design phase. Google's choice not to mandate encryption on its Android phones by default, for example, has led to a gap with Apple phones in terms of encryption, with only around 10% of Android phones encrypted at rest versus nearly 95% of iPhones.[273] Google has responded to this gap, with Android Q poised to require forms of encryption across its ecosystem.[274] These issues move beyond encryption and cover issues such as how devices are identified over time, how they integrate into other systems, and what data are gathered as part of quality control, each of which expose the user and the app to potential security attacks.[275]

Complicating factors further is the widespread redistribution of wearable hardware data from the cloud systems of the hardware companies. Some hardware companies like Fitbit encourage users to access, share, and redistribute their own data, without discussions of how that access and redistribution can re-identify users via the mosaic effect.[276] This leads to outcomes such as Strava's open data portal revealing the location of secret military bases via exercise patterns – with those devices now being banned for deployed troops.[277] These data are also often widely re-sold or shared with third parties such as insurance plans,[278] where they can represent emergent attack vectors for re-identification over time [279] (early research indicates only six days of full step counts are sufficient to re-identify an individual out of 100,000,000 participants).[280]

Recommendations for Consumer Technology Companies and App Developers

6-1. Google should join Apple in requiring a signed informed consent document for any mobile health research applications emerging from the use of ResearchStack.

6-2. Apple and Google should require developers to upload IRB approval letters as PDFs, and make those documents available in-line to consumers contemplating installing a mobile research app. This disclosure requirement is compatible with both traditional institutional review and with unregulated research where there is more than minimal risk.[281]

6-3. Apple and Google should implement and enforce a "floor" for privacy policies and terms of use. For example, such a floor could include provisions that no data may be transferred to third parties without specific consent for each use.[282]

6-4. Developers of research apps should leverage the existing, community-standard toolkits, such as ResearchKit and ResearchStack, each of which contains informed consent workflows and developer tools. These apps should (1) accommodate independent review when required by the app store platforms; (2) allow for isolation of malicious code elements; (3) publish a "software bill of materials" for any code integrated from a repository such as GitHub; and (4) publish a privacy disclosure notice."[283]

6-5. Makers of wearable devices should implement encryption both for data at rest and in transit. We further encourage federal and state investment in fundamental encryption research and development to support encryption on wearables that is easier to include for developers without overly damaging battery performance.

6-6. Security also must be implemented once the data have left the wearable and moved to the consumer's phone (or directly to the servers of the wearable company), and therefore we recommend that manufacturers of wearables adhere to basic cybersecurity practices. [284]

H. Organizations of Unregulated Researchers

As previously mentioned, unregulated researchers include citizen scientists, DIY researchers, self-experimenters, and patient-based research networks that promote research among their members. Terms such as citizen scientist and DIY researcher originally signified that researchers were amateurs or lay-people conducting research without scientific training and outside of traditional research settings. Today, however, they also include individuals with scientific backgrounds working outside of traditional research settings, not-for-profit patient and research organizations, and corporate entities.[285] Unregulated researchers may work independently, out of their homes or in community laboratories, or they may work in collaboration with more traditional regulated researchers.[286] Some unregulated researchers, such as self-experimenters and crowd-sourcing data suppliers, may passively or actively participate in unregulated research efforts,[287] giving existing mobile-platform data about themselves or collecting or generating new data via a mobile-platform to unregulated researchers. Previous research has shown that unregulated researchers are a heterogeneous group with varying degrees of relationship with regulated researchers and regulators.[288]

Although entities covered by the Common Rule have developed fairly uniform conceptions of the privacy protections and risks of participation in research with human participants, unregulated researchers and unregulated research organizations may consider the elements of traditional research ethics differently than regulated researchers.[289] For instance, some unregulated researchers may value speed or openness of data collection and management to answer research questions over privacy of individual participants or eschew research funding so long as research questions can be answered efficiently.[290] While they may lack a common vocabulary or set of values with regard to best practices for mobile health research, some shared features of citizen

science organizations are their reliance on information communication technologies to collect, supply, and analyze data, crowdsourcing research participation, and "grassroots" strategies to fund research.[291]

Some organizations of unregulated researchers (e.g., PatientsLikeMe, Quantified Self, and the Citizen Science Association) are well positioned to promote best practices for mobile health-based research through education. For example, in 2011, DIYBio published a Draft Code of Ethics, including provisions regarding open access, transparency, education, and safety.[292] These organizations also may serve as liaisons between the NIH, regulatory bodies, app developers, research participants, and individual unregulated researchers.

The following recommendations propose that organizations of unregulated researchers should assume a greater role in educating and guiding their members about research.

Recommendations for Organizations of Unregulated Researchers

7-1. Organizations of researchers conducting studies in unregulated environments, such as community organizations, member associations, and patient research networks, should adopt guidance and/or standards for their members, including on the following issues:

a. Guidance on how best to transparently communicate the goals, risks, benefits, and data handling procedures of their research prior to enrolling a participant.

b. Guidance on privacy policies and terms of service for mobile device-based research.

c. Guidance on the privacy policies and terms of service of third party developed devices or apps.

IV. Conclusion

The general legal and ethical provisions for research with human participants in most of the world are easy to summarize. All researchers are legally required and ethically compelled to adhere to established rules and norms of research ethics. Thus, for example, researchers must minimize risks and maximize benefits to participants, participants must provide knowing and voluntary informed consent, and a research ethics committee must approve the research protocol. Things are more complicated in the United States, where federal research regulations apply to most, but not all, research. In the handful of states that have their own research laws, almost all of them are limited in scope, protections, or both. Thus, there is a discrete and growing category of "unregulated" research.

Recent technological and societal developments in the U.S. have increased the amount of unregulated research performed, although there are no estimates available on the amount of unregulated research or number of unregulated researchers. The widely assumed increase in unregulated research is attributable to, among other things, development of research apps for smartphones and other mobile devices, availability of direct-to-consumer genetic and other biomedical testing, formation of social media groups interested in health research, and growth of big data analytics for compilation and analysis of diverse data sets. The societal concern is that some unregulated research, mostly conducted by citizen scientists and others without formal training in scientific research, may be of low quality and suffer from a lack of ethics review, fail to adhere to generally recognized ethical norms for the treatment of research participants, and result in findings that expose research participants or larger groups of individuals (e.g., those with certain health conditions) to a range of harms from privacy violations to psychological and physical injury.

Extending federal research regulations to cover all research with human participants would be the easiest and most effective way to address the problem, but it is not viable politically and therefore it would be pointless to recommend. We also reject the view that the current laissez faire approach to unregulated research should be retained. Our preferred, middle ground option, is a suite of measures including education, consultation, transparency, self-governance, and regulation to ensure the quality of unregulated research and inform researchers and potential participants about key issues in research ethics. Our recommendations are directed to state governments, federal agencies, technology companies, app developers, and organizations of unregulated researchers.

The ethical bases of our recommendations are widely respected research ethics pronouncements in the U.S. (e.g., Belmont Report) and internationally (e.g., Nuremberg Code, Declaration of Helsinki). The unifying characteristic of our recommendations is pragmatism. We believe that our recommendations are realistic, feasible, and likely to produce positive results. They are also designed to be freestanding. Thus, even if all of our recommendations are not adopted, the adopted ones will make a valuable contribution to the conduct of unregulated health research using mobile devices. At the same time, implementation will require coordination and oversight to ensure that the multiple entities giving force to the recommendations do not establish conflicting regimes.

References:

[1] The White House, The Precision Medicine Initiative, *available at* https://obamawhitehouse.archives.gov/precision-medicine (last visited July 15, 2019).

[2] Electronic Medical Records and Genomics (eMerge) Network, *available at* https://www.genome.gov/Funded-Programs-Projects/Electronic-Medical-Records-and-Genomics-Network-eMERGE (last visited July 15, 2019).

[3] M. Angrist, "Eyes Wide Open: The Personal Genome Project, Citizen Science and Veracity in Informed Consent," *Personalized Medicine* 6, no. 6 (2009): 691-699.

[4] J. Woolley et al., "Citizen Science or Scientific Citizenship? Disentangling the Uses of Public Engagement Rhetoric in National Research Initiatives," *BMC Medical Ethics* 17:33 (2016); M.A. Rothstein, "Ethical Issues in Big Data Health Research," *Journal of Law, Medicine & Ethics* 43, no. 2 (2015): 425-429.

[5] A. Wiggins and J. Wilbanks, "The Rise of Citizen Science in Health and Biomedical Research," *American Journal of Bioethics* 19, no. 8 (2019): 3-14. *See also* C.J. Guerrini et al., "Biomedical Citizen Science or Something Else? Reflections on Terms and Definitions," *American Journal of Bioethics* 19, no. 8 (2019): 17-19; H. Riesch and C. Potter, "Citizen Science as Seen by Scientists: Methodological, Epistemological and Ethical Dimensions," *Public Understanding of Science* 23, no. 1 (2013):107-120.

[6] S. Hoffman, "Citizen Science: The Law and Ethics of Public Access to Medical Big Data," *Berkeley Technology Law Journal* 30, no. 3 (2015): 1741-1805; F. Khatib et al., "Algorithm Discovery by Protein Folding Game Players," Proceedings of the National Academy of Science 108, no. 47 (2011): 18949-18953; A. Irwin, "Science, Public Engagement," In: J.D. Wright, ed., *International Encyclopedia of the Social and Behavioral Sciences*. (Oxford: Elsevier, 2015), 255–260; M. McGowan et al., "'Let's Pull These Technologies Out of the Ivory Tower': The Politics, Ethos, and Ironies of Participant-driven Genomic Research," *BioSocieties* 12, no. 4 (2017): 494-519.

[7] B.J. Evans, "Parsing the Line between Professional and Citizen Science," *American Journal of Bioethics* 19, no. 8 (2019): 15-17; A. Fiske, B. Prainsack, and A. Buyx, "Meeting the Needs of Underserved Populations: Setting the Agenda for More Inclusive Citizen Science of Medicine," *Journal of Medical Ethics* 45, no. 9 (2019): 617-622.

[8] *See* M.A. Rothstein, J.T. Wilbanks, and K.B. Brothers, "Citizen Science on Your Smartphone: An ELSI Research Agenda," *Journal of Law, Medicine & Ethics* 43, no. 4 (2015): 897-903.

[9] *See, e.g.*, J. Berkelman, Y. Li, and C.P. Gross, "Scope and Impact of Financial Conflicts of Interest in Biomedical Research: A Systematic Review," *Journal of the American Medical Association* 289, no. 4 (2003): 454-465; P. Trouiller et al., "Drug Development for Neglected Diseases: A Deficient Market and a Public-Health Policy Failure," *The Lancet* 359, no. 9324 (2002): 2188-2194; M. Walsh, G. Grant, and Z. Coleman, "Action Research – A Necessary Complement to Traditional Health Science?" *Health Care Analysis* 16, no. 2 (2008): 127-144.

[10] Wiggins and Wilbanks, *supra* note 5; M. Swan, "Crowdsourced Health Research Studies: An Important Emerging Complement to Clinical Trials in the Public Health Ecosystem," *Journal of Medical Internet Research* 14, no. 2 (2012): e46, DOI: 10.2196/jmir.1988.

[11] *See, e.g.*, P. Beresford, "Developing the Theoretical Basis for a Service User/Survivor-Led Research and Equal Involvement in Research," *Epidemiology and Psychiatric Services* 14, no. 1 (2005): 4-9; G. Seyfried, L. Pei, and M. Schmidt, "European Do-It-Yourself (DIY) Biology: Beyond the Hope, Hype and Horror," *BioEssays* 36, no. 6 (2014): 548-551.

[12] John T. Wilbanks, Co-PI on the grant reported in this article and co-author of this article, is the Chief Commons Officer of Sage Bionetworks.

[13] McGowan et al., *supra* note 6.

[14] *Id.*; D.B. Resnik, "Citizen Scientists as Human Subjects: Ethical Issues," *Citizen Science: Theory and Practice* 4(1) no. 11 (2019): 1-7, doi: https://doi.org/10.5334/cstp.150.

[15] 45 U.S.C. § 3724. *See* Helping Federal Agencies Accelerate Innovation through Public Participation, *available at* https:/www.citizenscience.gov/# (last visited October 7, 2019).

[16] Pub. L. 114-255 (2016).

[17] Section 3022 of the 21st Century Cures Act provides that real world evidence may be based on "ongoing safety surveillance, observational studies, registries, claims, and patient-centered outcomes research activities." *See* R.E. Sherman et al., "Real World Evidence – What Is It and What Can It Tell Us?" *New England Journal of Medicine* 375, no. 23 (2016): 2293-2297.

[18] For a discussion of the study's methodology, *see* M.A. Rothstein and J.T. Wilbanks, "Unregulated Health Research Using Mobile Devices: Introduction," *Journal of Law, Medicine & Ethics* 48, no. 1 (Supp.) (2020): ____.

[19] *See* Parts I-B and III-B *infra*.

[20] See M. Doerr and C. Guerrini, "Who Are the People in Your Neighborhood? Personas Populating Unregulated mHealth Research," *Journal of Law, Medicine & Ethics* 48, no. 1 (Supp.) (2020): _____.

[21] The 16 Common Rule Departments and Agencies and their regulations are as follows: Department of Homeland Security, 6 C.F.R. Pt. 46; Department of Agriculture, 7 C.F.R. Pt. 1c; Department of Energy, 10 C.F.R. Pt. 745; National Aeronautics and Space Administration, 14 C.F.R. Pt. 1230; Department of Commerce, 15 C.F.R. Pt. 27; Social Security Administration, 20 C.F.R. Pt. 431; Agency for International Development, 22 C.F.R. Pt. 225; Department of Housing and Urban Development, 24 C.F.R. Pt. 60; Department of Labor, 29 C.F.R. Pt. 21; Department of Defense, 32 C.F.R. Pt. 219; Department of Education, 34 C.F.R. Pt. 97; Department of Veterans Affairs, 38 C.F.R. Pt. 16; Environmental Protection Agency, 40 C.F.R. Pt. 26; Department of Health and Human Services, 45 C.F.R. Pt. 46; National Science Foundation, 45 C.F.R. Pt. 690; Department of Transportation, 49 C.F.R. Pt. 11. The Department of Justice and the Consumer Product Safety Commission intend to be signatories to the 2018 Common Rule, and the Central Intelligence Agency and the Office of the Director of National Intelligence follow the Common Rule pursuant to Executive Orders. For a further discussion, *see* M.N. Meyer, "There Oughta Be a Law: When Does(n't) the U.S. Common Rule Apply?," *Journal of Law, Medicine & Ethics* 48, no. 1 (Supp.) (2020): ___.

[22] Food and Drug Administration, Protection of Human Subjects, 21 C.F.R. Pt. 50.

[23] Section 5(a) of the Federal Trade Commission Act, 15 U.S.C. § 45, prohibits "unfair or deceptive acts or practices in or affecting commerce."

[24] Pub. L. 104-191 (1996); 45 C.F.R. Pts. 160, 164.

[25] Pub. L. 111-5 (2009); 74 Fed. Reg. 56123-56131.

[26] *See* Part III-C *infra*.

[27] 45 C.F.R. § 46.102(l) (Department of Health and Human Services). In some cases, mobile health blurs the lines between research and other activities, such as product development, marketing, and quality improvement.

[28] 45 C.F.R. § 46.102(e) (Department of Health and Human Services).

[29] For examples of various types of unregulated researchers, *see* Doerr and Guerrini, *supra* note 20. For use cases of unregulated research using mobile devices, see *infra* section I-D.

[30] J.L. Dickinson, B. Zuckerberg, and D.N. Bonter, "Citizen Science as an Ecological Research Tool: Challenges and Benefits," *Annual Review of Ecology, Evolution, and Systematics* 41, no. 1 (2010): 149-172.

[31] K.V. Kreitmair and D.C. Magnus, "Citizen Science and Gamification," *Hastings Center Report* 49, no. 2 (2019): 40-46.

[32] *See* E. Pauwels and S.W. Denton, *The Rise of the Bio-Citizen*, T. Kuiken, ed. (2018): 47-57, *available at* https://www.wilsoncenter.org/sites/default/files/rise_of_biocitizenfinal.pdf (last visited September 13, 2019).

[33] Pew Research Center, "Global Attitudes Project, Smartphone Ownership Is Growing Around the World, But Not Always Equally," February 5, 2019, *available at* https://www.pewresearch.org/global/2019/02/05/smartphone-ownership-is-growing-rapidly-around-the-world-but-not-always-equally (last visited September 4, 2019). *See generally* I. Sim, "Mobile Devices and Health," *New England Journal of Medicine* 381, no. 10 (2019): 956-968.

[34] A. Edwards, "Health: Health Care Mobile App Trends in 2019," *Ortholive Blog*, February 2, 2019, *available at* www.ortholive.com/blog/ealth-healthcare-mobile-app-trends-in-2019 (last visited September 1, 2019).

[35] M. Pohl, "325,000 Mobile Health Apps Available in 2017 – Android Now the Leading Mobile Health Platform," Research 2 Guidance, 2017, *available at* https://research2guidance.com/325000-mobile-health-apps-available-in-2017 (last visited September 1, 2019). For a discussion of the privacy risks created by many of the health apps, *see* L. Andrews, "A New Privacy Paradigm in the Age of Apps," *Wake Forest Law Review* 53, no. 3 (2018): 421-478.

[36] C. Nebeker, "mHealth Research Applied to Regulated and Unregulated Behavioral Health Sciences," *Journal of Law, Medicine & Ethics* 48, no. 1 (Supp.) (2020): _____.

[37] Z. Chu and M. Majumdar, "Why Apple's ResearchKit Signals a Golden Age for Health Care," *Fortune*, March 27, 2015, *available at* https://fortune.com/2015/03/27/why-apples-researchkit-signals-a-golden-age-for-health-care/ (last visited July 12, 2019).

[38] A. Duhaime-Ross, "Apple's New ResearchKit: 'Ethics Quagmire' or Medical Research Aid?" *The Verge*, March 10, 2015, *available at* https://www.theverge.com/2015/3/10/8177683/apple-research-kit-app-ethics-medical-research (last visited July 12, 2019).

[39] V. Tourraine, "List of All ResearchKit Apps (from Science, February 1, 2016)," *available at* http://blog.shazino.com/articles/science/researchkit-list-apps/ (last visited July 12, 2019).

[40] S. Moore et al., "Consent Processes for Mobile App Mediated Research: Systematic Review," *JMIR Mobile Health uHealth* 5, no. 8 (2017): doi:10.2196/ealth.7014.

[41] J. Naughton, "'The Goal Is to Automate Us': Welcome to the Age of Surveillance Capitalism," *The Guardian*, January 20, 2019, *available at* https://www.theguardian.com/technology/2019/jan/20/shoshana-zuboff-age-of-surveillance-capitalism-google-facebook (last visited July 12, 2019).

[42] C.M. Gray et al., "The Dark (Patterns) Side of UX Design," In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems (CHI '18)* (New York, N.Y., ACM, 2018), DOI: https://doi.org/10.1145/3173574.3174108.

[43] J. Obar and A. Oeldorf-Hirsch, "The Biggest Lie on the Internet: Ignoring the Privacy Policies and Terms of Service Policies of Social Networking Services," June 1, 2018, from TPRC 44: The 44th Research Conference on Communication, Information and Internet Policy, 2016, *available at* SSRN: https://ssrn.com/abstract=2757465 or http://dx.doi.org/10.2139/ssrn.2757465 (last visited July 12, 2019).

[44] 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 July 12, 2019).

[45] *See* A.M. McDonald and L.F. Cranor, "The Cost of Reading Privacy Policies," *I/S: A Journal of Law and Policy for the Information Society*, 2008 Privacy Year in Review, http://www.is-journal.org (noting the burden of reading privacy policies).

[46] Statcounter, Mobile Operating System Market Share, United States of America, May 2018-May 2019, *available at* http://gs.statcounter.com/os-market-share/mobile/united-states-of-america (last visited June 5, 2019).

[47] S. Vaidhyanathan, *The Googlization of Everything: (and Why We Should Worry)*. (Berkeley: University of California Press, 2012).

[48] T.B. Jorgensen, "Will 'Sign in with Apple' Revolutionize Digital Identity?" *Infosecurity Magazine*, July 11, 2019, *available at* https://www.infosecurity-magazine.com/opinions/sign-apple-digital-identity-1-1/ (last visited July 12, 2019).

[49] G.A. Fowler, "Review: Google Chrome Has Become Surveillance Software: It's Time to Switch," *Mercury News*, June 21, 2019, *available at* https://www.mercurynews.com/2019/06/21/google-chrome-has-become-surveillance-software-its-time-to-switch/ (last visited July 12, 2019).

[50] One way in which this difference is evident is in their approach to pornography. *See* Apple CEO Cook: We Don't Want Porn in Our App Store," MacDaily News, March 29, 2018, *available at*

https://macdailynews.com/2018/03/29/apple-ceo-cook-we-dont-want-porn-in-our-app-store/ (last visited July 12, 2019).

[51] K. Terry, "Apple Opens iPhone EHR Feature to All Health Care Organizations," *Medscape*, July 3, 2019, *available at* https://www.medscape.com/viewarticle/915208 (last accessed July 12, 2019).

[52] Carin Alliance, The Carin Alliance Code of Conduct, *available at* https://www.carinalliance.com/our-work/trust-framework-and-code-of-conduct/ (last accessed July 12, 2019).

[53] These issues are further discussed in section II-C *infra* and K.B. Brothers, E.W. Clayton, and A.J. Goldenberg, "Online Pediatric Research: Addressing Consent, Assent, and Parental Permission," *Journal of Law, Medicine & Ethics* 48, no 1 (Supp.) (2020): ____.

[54] S.M. Wolf, "Return of Results in Unregulated Research Using Mobile Devices," *Journal of Law, Medicine & Ethics* 48, no. 1 (Supp.) (2020): ___-____.

[55] *See* R. Bonney et al., "Next Steps for Citizen Science," *Science* 343, no. 6178 (2014): 1427-1436; A. Fiske et al., "Conceptual and Ethical Considerations for Citizen Science in Biomedicine," *Personal Health Science*, N.B. Heyen, S. Dickel, and A. Brüninghaus, eds. (Wiesbaden: Springer 2018): 195-217.

[56] E.J. Emanuel, D. Wendler, and C. Grady, "What Makes Clinical Research Ethical?" *Journal of the American Medical Association* 283, no. 20 (2000): 2701-2711; L. Hood and M. Flores, "A Personal View on Systems Medicine and the Emergence of Proactive P4 Medicine: Predictive, Preventive, Personalized and Participatory," *Nature Biotechnology* 29 (2012): 613-624.

[57] *See* Risk of Harms, *infra* Part I-F.

[58] E.A. Largent, H.F. Lynch, and M.S. McCoy, "Patient-Engaged Research: Choosing the "Right" Patients to Avoid Pitfalls," *Hastings Center Report* 48, no. 5 (2018): 26-34.

[59] A.C. Janssens and P. Kraft, "Research Conducted Using Data Obtained through Online Communities: Ethical Implications of Methodological Limitations," *Public Library of Science: Medicine* (2012), e1001328.

[60] L. Del Savio, B. Prainsack, and B. Buyx, "Motivations of Participants in the Citizen Science of Microbiomics: Data from the British Gut Project," *Genetics in Medicine* 19, no. 8 (2017): 959-961. *See also* S. Callier and S.M. Fullerton, "Diversity and Inclusion in Unregulated mHealth Research: Addressing the Risks," *Journal of Law, Medicine & Ethics* 48, no. 1 (Supp.) (2020): ___; Fiske et al., *supra* note 55.

[61] E. Vayena and J. Tasioulas, "Adapting Standards: Ethical Oversight of Participant-Led Research," *Public Library of Science: Medicine* (2013), doi: 10137/journal.pmed.1001402.

[62] D. Resnik, "Citizen Scientists as Human Subjects: Ethical Issues" (2019), *available at* https://theoryandpractice.citizenscienceassociation.org/article/10.5334/cstp.150print (last visited May 12, 2019).

[63] H. Riesch and C. Potter, "Citizen Science as Seen by Scientists: Methodological, Epistemological and Ethical Dimensions," *Public Understanding of Science* 23, no. 1 (2013): 107-120, 111.

[64] An area of increasing concern is the compelled use of wearable devices by employers and insurers to measure compliance and effects of fitness tracking devices.

[65] *See* J.H. Yu and E. Juengst, "Do Groups Have Moral Standing in Unregulated mHealth Research?" *Journal of Law, Medicine & Ethics* 48, no. 1 (Supp.) (2020): ____.

[66] N.A. Feraro, D.S. Morrell, and C.N. Burkhart, "Skin Scan: A Demonstration of the Need for FDA Regulation of Medical Apps on iPhone," *Journal of the American Academy of Dermatology* 68, no. 3 (2013): 515-516.

[67] K. Huckvale et al., "Smartphone Apps for Calculating Insulin Dose: A Systematic Assessment," *BMC Medicine* 13 (2015): 106.

[68] U.S. Food and Drug Administration, FDA Warns against the Use of Unauthorized Devices for Diabetes Management (May 17, 2019), *available at* https://www.fda.gov/news-events/press-announcements/fda-warns-against-use-unauthorized-devices-diabetes-management (last visited June 3, 2019).

[69] K.G. Baron et al., "Are Some Patients Taking the Quantified Self Too Far?," *Journal of Clinical Sleep Medicine* 13, no. 2 (2017): 351-354; B.X. Chen, "Data that May Keep You Up at Night: Sleep-tracking Apps and Devices Can't Cure Your Insomnia, and They Could Even Make It Worse," *New York Times*, July 18, 2019, at B6.

[70] P.G. Turner and C.E. Lefevre, "Instagram Use is linked to Increased Symptoms of Orthorexia Nervosa," *Eating and Weight Loss Disorders* 22, no. 2 (2017): 277-284.

[71] C.C. Simpson and S.E. Mazzeo, "Calorie Counting and Fitness Tracking Technology: Associations with Eating Disorder Symptomatology," *Eating Behaviors* 26, no. 1 (2017): 89-92.

[72] *See, e.g.*, J. Wakefield, "Sex Lives of App Users 'Shared with Facebook,'" *available at* https://www.bbc.com/news/technology-49647239 (last visited September 13, 2019) (fertility/menstrual tracking apps shared data about sexual activity with Facebook).

[73] 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. Doi:10.1001/jamanetworkopen.2019.2542.

[74] S.R. Blenner et al., Privacy Policies of Android Diabetes Apps and Sharing of Health Information," 315 *Journal of the American Medical Association* 315, no. 10 (2016): 1051-1052.

[75] D.G. Smith, "Mental Health Apps Are Scooping Up Your Most Sensitive Data. Will You Benefit?" *STAT*, September 20, 2019, *available at* https://www.statnews.com/2019/09/20/mental-health-apps-capture-sensitive-data (last visited September 20, 2019).

[76] *Id.*

[77] A. McDonald, J. McDonnell, and C. Mitchell, "Mobile Apps: Redefining the Virtual California Economy and the Laws that Govern It," *Competition: Journal of the Antitrust and Unfair Competition Law Section of the State Bar of California* 24, no. 2 (2015): 86, 88.

[78] P. Schaffer, "Data Breaches on the Rise: How Healthcare Organizations Can Protect against Medical Identity Theft," *Digital Health News*, July 3, 2018, *available at* https:www.idigitalhealth.com/news/data-breaches-on-the-rise-how-healthcare-organizations-can-protect-against-medical-identity-theft.

[79] H. Dongjing et al., "Security Concerns in Android Mobile Health Apps," *AMIA Annual Symposium Proceedings* 2014 (2014): 645-654.

[80] A.C. Janssens and P. Kraft, "Research Conducted Using Data Obtained through Online Communities: Ethical Implications of Methodological Limitations, *Public Library of Science: Medicine* (2012): 9, e1001328. *See generally* A. Fiske et al., "Conceptual and Ethical Considerations for Citizen Science in Biomedicine," in N.B. Heyen, S. Dickel, and A. Bruninghaus, eds., *Personal Health Science* (Wiesbaden, Germany: Springer 2018): 195-217.

[81] *See* M.A. Majumder and A.L. McGuire, "Data Sharing in the Context of Health-Related Citizen Science," *Journal of Law, Medicine & Ethics* 48, no. 1 (2020): ___.

[82] Of course, even regulated research is subject to misleading characterization and dissemination on the internet.

[83] P.W. Armstrong and C.D. Naylor, "Counteracting Health (Mis)information: A Role for Medical Journals?" *Journal of the American Medical Association* 321, no. 19 (2019): 1863-1864; A. Kata, "Anti-vaccine Activists, Web 2.0, and the Postmodern Paradigm – An Overview of Tactics and Tropes Used Online by the Anti-vaccination Movement," *Vaccine* 30, no. 25 (2012): 3778-3789.

[84] C. Hauser, "Whatever Ails You, F.D.A. Says, Drinking Bleach Isn't the Answer," *New York Times*, August 14, 2019, at A19: B. Zadrozny, "Fake Science Led a Mom to Feed Bleach to Her Autistic Sons – and Police Did Nothing to Stop Her," NBS News Internet, June 14, 2019, *available at* https://www.nbcnews.com/tech/internet/fake-science-led-mom-fee-bleach-her-autistic-sons-police-n1017256 (last visited June 17, 2019).

[85] Department of Health and Human Services, Office for Human Research Protections, International Compilations of Human Research Standards (2019 ed.), *available at* https:www.hhs.gov/ohrp/sites/default/files/2019-International-Compilation-of-Human-Research-Standards.pdf (last visited April 17, 2019) (Canada, Finland, France, and many other countries regulate all research without regard to funding source).

[86] *See* L.M. Rasmussen, "Filling the 'Ethics Gap' in Citizen Science Research: A Workshop Report" (2016), *available at* https://www.niehs.nih.gov/research/supported/translational/peph/webinars/ethics/rasmussen_508.pdf (last visited May 12, 2019).

[87] Unregulated research also raises a wide range of issues normally referred to as "scientific integrity," including research misconduct, conflicts of interest, sharing data and samples, assigning authorship, and acting in a socially responsible manner. *See* D.B. Resnik, "Citizen Scientists as Human Subjects: Ethical Issues," *available at* https://theoryandpractice.citizenscienceassociation.org/articles/10.5334/cstp.150/print (last visited May 12, 2019). These issues are beyond the scope of this research project.

[88] National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research, *The Belmont Report: Ethical Principles and Guidelines for the Protection of Human Subjects of Research* (Washington, DC: US Gov't Printing Office, 1979): section B-2.

[89] N.M. King, "Defining and Describing Benefit Appropriately in Clinical Trials," *Journal of Law, Medicine & Ethics* 28, no. 2 (2000): 332-343.

[90] P.B. Miller and C. Weijer, "Rehabilitating Equipoise," *Kennedy Institute of Ethics Journal* 13, no. 2 (2003): 93-118.

[91] R.S. Nickerson, "Confirmation Bias: A Ubiquitous Phenomenon in Many Guises," *Review of General Psychology* 2, no. 2 (1998): 175-220.

[92] *Belmont Report*, *supra* note 88.

[93] 45 C.F.R. § 46.116.

[94] I. Albala, M. Doyle, and P.S. Appelbaum, "The Evolution of Consent Forms for Research: A Quarter Century of Changes," *IRB* 32, no. 3 (2010): 7-11; M.K. Paasche-Orlow et al., "Readability of Consent Form Templates: A Second Look," *IRB* 35, no. 4 (2013): 12-19; E. Larson, G. Foe, and R. Lally, "Reading Level and Length of Written Research Consent Forms," *Clinical and Translational Science* 8, no. 4 (2015): 355-356.

[95] W. Montalvo and E. Larson, "Participant Comprehension of Research for Which They Volunteer: A Systematic Review," *Journal of Nursing Scholarship* 46, no. 6 (2014): 423-431.

[96] *Id.*; A. Nishimura et al., "Improving Understanding in the Research Informed Consent Process: A Systematic Review of 54 Interventions Tested in Randomized Control Trials," *BMC Medical Ethics* 14 (2018): 28; L. Tamariz et al., "Improving the Informed Consent Process for Research Subjects with Low Literacy: A Systematic Review," *Journal of General Internal Medicine* 28, no. 1 (2013): 121-126.

[97] C.M. Hammack-Aviran, K.M. Brelsford, and L.M. Beskow, "Ethical Considerations in the Conduct of Unregulated Mobile Health Research," *Journal of Law, Medicine & Ethics* 48, no. 1 (Supp.) ___ (2020).

[98] *Id.*

[99] N.A. Garrison et al., A Systematic Literature Review of Individuals' Perspectives on Broad Consent and Data Sharing in the United States," *Genetics in Medicine* 18, no. 7 (2016): 663-671; Steinsbekk KS, B Myskja, and B. Solberg, "Broad Consent Versus Dynamic Consent in Biobank Research: Is Passive Participation an Ethical Problem?" *European Journal of Human Genetics* 21, no. 9 (2013): 897-902.

[100] J.R. Ridpath, S.M. Greene, and C.J. Wiese, "PRISM Readability Toolkit – 2007," *available at* https://www.kpwashingtonresearch.org/about-us/capabilities/research-communications/prism/. (last visited February 22, 2019).

[101] Agency for Health Research and Quality, Informed Consent, *available at* https://www.ahrq.gov/funding/policies/informedconsent/index.html (last visited August 30, 2019).

[102] Hammack-Aviran, Brelsford, and Beskow, *supra* note 97.

[103] Sage Bionetworks, Toolkits for Informed Consent, and Mobile Research Studies, *available at* https://sagebionetworks.org/tools_resources/elements-of-informed-consent/ (last visited August 30, 2019); https://sagebionetworks.org/tools_resources/privacy-toolkit-for-mobile-health-research-studies/ (last visited August 30, 2019).

[104] M. Doerr et al., "Formative Evaluation of Participant Experience with Mobile eConsent in the App-Mediated Parkinson mPower Study: A Mixed Methods Study," *Journal of Medical Informatics Research Mobile Health Uhealth.* 5, no. 2 (2017): e14.

[105] J. Wilbanks, "Electronic Informed Consent in Mobile Applications Research," *Journal of Law, Medicine & Ethics* 48, no. 1 (Supp.) (2020): ___. *See also* S.R. Cummings and M.C. Rowbotham, "Electronic Informed Consent and Internet-Based Trials," *New England Journal of Medicine* 376, no. 9 (2017): 859-861; M.V. McConnell and E.A. Ashley, "Mobile Health Research – App-Based Trials and Informed Consent," *New England Journal of Medicine* 376, no. 9 (2017): 861-863.

[106] World Medical Association, *Declaration of Helsinki*, General Principles, ¶9 (1964).

[107] *Id*., Preamble, ¶2.

[108] *Id*.

[109] Council for International Organizations of Medical Sciences, *International Ethical Guidelines for Health-Related Research Involving Humans*, Guideline 22 (4th ed. 2016) ("Use of Data Obtained from the Online Environment and Digital Tools in Health-Related Research").

[110] *Id*.

[111] *Id*.

[112] *Id*.

[113] 45 C.F.R. § 46.111(a)(7).

[114] *See id*. § 160.103 (defining covered entity to include a health plan, a health care clearinghouse, and a health care provider that transmits any health information in electronic form in connection with a standard transaction); U.S. Department of Health and Human Services, *Protecting Personal Health Information in Research: Understanding the HIPAA Privacy Rule* (2003): 1-37 ("In some instances, researchers may have to comply with the Privacy Rule because they may be or may work for a covered entity. For example, the Privacy Rule defines covered entities to include health care providers that transmit health information electronically in connection with certain financial and administrative transactions (such as most hospitals). As such, researchers who are or who work for these covered entities would need to understand the Privacy Rule . . .").

[115] 45 C.F.R. §§ 164.502-.514.

[116] *Id*. §§ 164.520-.528.

[117] *Id*. § 164.530.

[118] *Id*. § 164.508(a)(1) (establishing the prior written authorization requirement); *id*. § 164.512(i)(1)(i)-(iii) (establishing three research-related exceptions to the authorization requirement); *id*. § 164.514(e) (establishing a fourth research-related exception to the authorization requirement for limited research data sets). Some state laws also impose privacy and security obligations on certain researchers. For example, Texas law requires researchers not regulated by the HIPAA Privacy Rule to provide notice and obtain authorization before electronically disclosing an individual's PHI, refrain from using or disclosing an individual's PHI for certain marketing activities unless the individual gives "clear and unambiguous" written or electronic permission, refrain from disclosing an individual's PHI in exchange for direct or indirect remuneration and complete privacy training. Tex. Health & Safety Code §§ 181. 101, .152-154.

[119] *Id*. § 164.308.

[120] *Id*. § 164.310.

[121] *Id*. § 164.312.

[122] *Id*. § 164.306(a)(1)-(2).

[123] *Id*. §§ 164.400-.414.

[124] 45 C.F.R. Part 46B (pregnant women, human fetuses and neonates involved in research); 45 C.F.R. Part 46C (prisoners); 45 C.F.R. Part 46D (children).National Institutes of Health, Vulnerable and Other Populations

Requiring Additional Protection, *available at* https://grants.nih.gov/policy/humansubjects/policies-and-regulations/vulnerable-populations.htm (last visited September 2, 2019).

[125] *See* C.H. Coleman, "Vulnerability as a Regulatory Category in Human Subject Research," *Journal of Law, Medicine & Ethics* 37, no. 1 (2009): 12-18; J. Metcalf and K. Crawford, "Where Are Human Subjects in Big Data Research? The Emerging Ethics Divide," *Big Data & Society* (2016): 1-4, DOI: 10.1177/2053951716650211.

[126] Council for International Organizations of Medical Sciences, *International Ethical Guidelines for Health-Related Research Involving Humans*, Guideline 22 (4th ed. 2016) ("Use of Data Obtained from the Online Environment and Digital Tools in Health-Related Research").

[127] Brothers, Clayton, and Goldenberg, *supra* note 53.

[128] M. Anderson, "Racial and Ethnic Differences in How People Use Mobile Technology," *Pew Research Center* (2015), *available at* https://www.pewresearch.org/fact-tank/2015/04/30/racial-and-ethnic-differences-in-how-people-use-mobile-technology (last visited September 2, 2019); O. Sylvain, "Network Equality." *Hastings Law Journal* 67, no. 3 (2015): 443-497. On the issue of group harms, *see* Yu and Juengst, *supra* note 65.

[129] K. Montgomery, J. Chester, and K. Kopp, "Health Wearable Devices in the Big Data Era: Ensuring Privacy, Security, and Consumer Protection," *Center for Digital Democracy Report* (2016), *available at* *https://www.democraticmedia.org/sites/default/files/field/public/2016/aucdd_wearablesreport_final121516.pdf* (last visited September 2, 2019); J.T. Senders et al., "The Ethics of Passive Data and Digital Phenotyping in Neurosurgery," in M.L.D. Broekman ed., *Ethics of Innovation in Neurosurgery* (Switzerland: Springer, 2019): 129-141.

[130] R. Reyes et al., "Where Is the Community Dimension in the Updated Common Rule?" *Progress in Community Health Partnerships: Research, Education, and Action* 12, no. 1 (2018): 83-87.

[131] World Medical Association, Declaration of Helsinki – Ethical Principles for Medical Research Involving Human Subjects, *available at* https://www/wma.net/policies-post/wma-declaration-of-helsinki-ethical - principles-for-medical-research-involving-human-subjects (last visited August 14, 2019).

[132] C. Grady, "Institutional Review Boards: Purposes and Challenges, *Chest* 148, no. 5 (2015): 1148-1155.

[133] 45 C.F.R. § 46.111.

[134] D. Forster, "Independent Institutional Review Boards," *Seton Hall Law Review* 32, no. 3 (2003): 513-523.

[135] L.M. Beskow et al., "Expert Perspectives on Oversight for Unregulated Mobile Health Research: Empirical Data and Commentary," *Journal of Law, Medicine & Ethics* 48, no. 1 (Supp.) (2020): ___-___.

[136] E.J. Emanuel, D. Wendler, and C. Grady, "What Makes Clinical Research Ethical?" *Journal of the American Medical Association* 283, no. 20 (2000): 2701-2711.

[137] *See* P. Friesen, B. Redman, and A. Caplan, "Of Straws, Camels, Research Regulations, and IRBs," *Therapeutic Innovation & Regulatory Science* 53, no. 4 (2019): https://doi.org/10/1177/2168479018783740.

[138] E.J. Emanuel et al., "Oversight of Human Participants Research: Identifying Problems to Evaluate Reform Proposals," *Annals of Internal Medicine* 141, no. 4 (2004): 282-291.

[139] C. Nebeker et al., "Ethical and Regulatory Challenges of Research Using Pervasive Sensing and Other Emerging Technologies," *American Journal of Bioethics Empirical Bioethics* 8, no. 4 (2017): 266-276.

[140] L.M. Beskow et al., *supra* note 135.

[141] National Research Council, "Guiding Principles for Scientific Inquiry," in *Scientific Research in Education* (Washington, DC: The National Academies Press, 2002): 50-79.

[142] S.G. Nicholls et al., "Reporting Transparency: Making the Ethical Mandate Explicit," *BMC Medicine* [Internet] 14, no. 1 (2016): 44, *available at* https://doi.org/10.1186/s12916-016-0587-5 (last visited September 4, 2019). *See generally* A.E. Shamoo and D.B. Resnik, *Responsible Conduct of Research*, 4th ed. (New York: Oxford University Press, 2015).

[143] B.C. Martinson, M.S. Anderson, and R. de Vries, "Scientists Behaving Badly," *Nature* 435, no. 7043 (2005): 737-738.

[144] National Academies of Sciences, Engineering, and Medicine. *Open Science by Design: Realizing a Vision for 1st Century Research* (Washington, DC: The National Academies Press, 2018).

[145] World Health Organization, Code of Conduct for Responsible Research 2017, *available at* https://www.who.int/about/ethics/code-of-conduct-responsible-research.pdf (last visited September 4, 2019).

[146] B. Woods, A. Coravos, and J.D. Corman, "The Case for a Hippocratic Oath for Connected Medical Devices," *Journal of Medical Internet Research* 21, no. 3 (2019):e12568. DOI: 10.2196/12568.

[147] *See, e.g.,* L.H. Newman, "A New Pacemaker Hack Puts Malware Directly on the Device," *Wired,* August 9, 2018, *available at* https://www.wired.com/story/pacemaker-hack-malware-black-hat/ (last visited September 4, 2019).

[148] Guiding Principles on Ethics in Digital Health Produced During a Seminar at Stanford Libraries, Feb. 21, 2019, *available at* http://library.stanford.edu/node/156021 (last visited July 9, 2019).

[149] A.D. Grant, G.I. Wolf, and C. Nebeker, "Approaches to Governance of Participant-led Research: A Qualitative Case Study," *British Medical Journal Open* 9:e025633.doi:10.1136/bmjopen-2018-025633 (2019).

[150] S.J. Lynn et al., "Designing a Platform for Ethical Citizen Science: A Case Study of CitSci.org," *Citizen Science: Theory and Practice* 4(1) (2018); Grant, Wolf, and Nebeker, *supra* note 149.

[151] Grant, Wolf, and Nebeker, *supra* note 149.

[152] *Id.* at 9.

[153] Lynn et al., *supra* note 150.

[154] J.P. Woolley et al., "Citizen Science or Scientific Citizenship? Disentangling the Uses of Public Engagement Rhetoric in National Research Initiatives," *BMC Medical Ethics* 2016 Dec; 17(1):33.

[155] Vayena and Tasioulas, *supra* note 61.

[156] *Id.*

[157] *Id*. A related source of ethical frameworks is the cybersecurity research community. The Hippocratic Oath for Connected Medical Devices "describes commitments to capabilities that preserve patient safety, as well as trust in the process of care delivery itself." I Am the Cavalry, Hippocratic Oath for Connected Medical Devices, *available at* https://iamthecavalry.org/oath (last visited August 14, 2019). *See* B. Woods, A. Corvasos, and J.D. Corman, "The Case for a Hippocratic Oath for Connected Medical Devices: Viewpoint," *Journal of Medical Internet Research* 21, no. 3 (2019), http://www.jmir.org/2019/3/e/2568.

[158] M. Lang, B.M. Knoppers, and M.H. Zawati, "International mHealth Research: Old Tools and New Challenges," *Journal of Law, Medicine & Ethics* 48, no. 1 (Supp.) (2020): ___; E.S. Dove and J. Chen, "To What Extent Does the EU General Protection Regulation (GDPR) Apply to Citizen Scientist-Led Health Research with Mobile Devices? *Journal of Law, Medicine & Ethics* 48, no. 1 (Supp.) (2020): ____.

[159] *See* McGowan et al., *supra* note 6.

[160] Department of Health and Human Services, Office for Human Research Protections, International Compilations of Human Research Standards (2019 ed.), *available at* https://www.hhs.gov/ohrp/sites/default/files/2019-International-Compilation-of-Human-Research-Standards.pdf (last visited April 17, 2019) (Canada, Finland, France, and many other countries regulate all research without regard to its source of funding).

[161] Unregulated researchers, such as citizen scientists and patient-directed researchers, lack the expertise and resources of academic medical centers and other government-funded entities.

[162] *See* § I-F, *supra.*

[163] "[C]itizen scientists are human, and like past human researchers, may not see or be tempted to ignore ethical issues in their work that oversight by others might have helped to identify." L.M. Rasmussen, "When Citizens Do Science: Stories from Labs, Garages, and Beyond," *Narrative Inquiry in Bioethics* 9, no. 1 (2019): 1-4, 2.

[164] *Cf.* Vayena and Tasioulas, *supra* note 61 (proposing a risk-based approach).

[165] National Research Act, Pub. L. 93-348, 88 Stat. 342 (1974).

[166] *See generally* J.H. Jones, *Bad Blood: The Tuskegee Syphilis Experiment* (New York: Free Press, expanded ed. 1993); A.M. Brandt, "Racism and Research: The Case of the Tuskegee Syphilis Experiment," *Hastings Center Report* 8, no. 6 (1978): 21-29.

[167] The National Research Act also established the National Commission for the Protection of Human Subjects in Biomedical and Behavioral Research. Its best known work was The Belmont Report, Ethical Principles and Guidelines for the Protection of Human Subjects of Research. Washington, DC: Department of Health, Education, and Welfare; DHEW Publication OS 78-0012 (1978), *available at* http://www.hhs.gov/ohrp/humansubjects/guidance/belmont.htm (last visited April 15, 2019).

[168] See note 21 *supra*.

[169] 21 C.F.R. Pt. 50. *See* Food and Drug Administration, Protection of Human Subjects; Informed Consent, 46 Fed. Reg. 8942 (1981).

[170] These federal wide assurances (FWAs), remain permissible on a voluntary basis in the revised Common Rule. Department of Homeland Security et al., Federal Policy for the Protection of Human Subjects: Final Rule, 82 Fed. Reg. 7149-7258, 7156 (2017).

[171] D.D. Federman, K.E. Hanns, and L.L. Rodriguez, eds., *Responsible Research: A Systems Approach to Protecting Research Participants* (Washington, DC: National Academies Press, 1993).

[172] National Bioethics Advisory Commission, *Ethical and Policy Issues in Research Involving Human Participants* (Bethesda, MD: 2001).

[173] Department of Homeland Security et al., Federal Policy for the Protection of Human Subjects: Final Rule, 82 Fed. Reg. 7149-7258 (2017).

[174] Department of Homeland Security et al., Federal Policy for the Protection of Human Subjects: Six Month Delay of the General Compliance Date of Revisions While Allowing the Use of Three Burden-Reducing Provisions During the Delay Period, 83 Fed. Reg. 28497 (2018).

[175] Department of Health and Human Services, Human Subjects Research Protections: Enhancing Protections for Research Subjects and Reducing Burden, Delay, and Ambiguity for Investigators: Advance Notice of Proposed Rulemaking, 76 Fed. Reg. 44512 (2011).

[176] Department of Homeland Security et al., Federal Policy for the Protection of Human Subjects: Notice of Proposed Rulemaking, 80 Fed. Reg.53933-54061 (2015).

[177] *Id.* at 53989-53992.

[178] Upon reflection on the perspectives expressed by these commenters, we were persuaded that the proposed extension of the Common Rule is not appropriate to include in a final rule at this time." Final Rule, *supra* note 164, at 7156.

[179] It is not clear whether the Common Rule departments and agencies currently have the statutory authority to do so or whether new federal legislation would be necessary, which would base the constitutional authority on the Commerce Clause or other part of the Constitution, rather than the Spending Clause. *See* M. Meyer, "The Common Rule and Mobile Health Research," *Journal of Law, Medicine & Ethics* 48, no. 1 (Supp.) (2020): ___.

[180] *See* S.A. Tovino, "Going Rogue: Mobile Research Applications and the Right to Privacy," *Notre Dame Law Review* 95, no. 1 (forthcoming 2019) (surveying state research laws and state data privacy, security, and breach notification laws); S.A. Tovino, "Mobile Research Apps and State Data Protection Statutes," *Journal of Law, Medicine, & Ethics* 48, no. 1 (Supp.) (2020): ____ (analyzing state research laws and state consumer privacy laws).

[181] Md. Code Ann., Health-Gen. §§ 13-2001--13-2004.

[182] *Id.* § 13-2002(b).

[183] *Id*. § 13-2002(a).

[184] *Id*. § 13-2002(a).

[185] *Id*. § 13-2001(b)(1) (italicized emphasis added).

[186] *See* New State Ice Co. v. Liebmann, 285 U.S. 262, 311 (1932) (Brandeis, J., dissenting) ("It is one of the happy incidents 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 country.").

[187] Va. Code Ann. §§ 32.1-162.16—32.1-162.20.

[188] *Id*. § 32.1-162.19(A).

[189] *Id*. § 32.1-162.19(B).

[190] *Id*. §§ 32.1-162.18(A), 32.1-162.19(B).

[191] N.Y. Pub. Health §§ 2440-2446.

[192] *Id*. § 2441(2).

[193] Cal. Health & Safety Code §§ 24170-24179.5.

[194] *Id*. § 24172.

[195] *Id*. §§ 24173, 24175.

[196] *Id*. § 24176.

[197] *Id*.

[198] 77 Ill. Admin. Code § 250.130(b)(1)(B).

[199] Wis. Stat. § 51.61(1)(a)(j).

[200] *Id*. § 51.61(1).

[201] Fla. Stat. Ann. § 381.026(4)(e).

[202] *Id*. § 381.026(4)(e).

[203] *See* Tovino, *supra* note 180 (surveying state data breach, security, and privacy statutes).

[204] *Id*.

[205] *Id*.

[206] *Id*.

[207] *Id*.

[208] *See, e.g.*, Ariz. Rev. Stat. § 20-448.02; Del. Code tit. 16, § 5175; Fla. Stat. § 760.40; Iowa Code § 729.6; Kan. Stat. § 65-4974; Mass. Gen. Laws § 70G; Mich. Comp. Laws §§ 333.17020, 333.17520; Miss. Code § 41-41-17; Neb. Rev. Stat. § 71-551; Nev. Rev. Stat. § 629.101 to .201; N.H. Rev. Stat. ch. 141-H:2; N.M. Sta. § 24-21-7; N.Y. Ins. Law § 2615; S.C. Code § 38-93-50.

[209] *See, e.g.*, Fla. Stat. § 760.40; Ill. Comp. Stat. ch. 410, § 1-50; Me. Stat. tit. 22, § 1711-C; N.J. Stat. § 10:15-43 to -49; Okla. Stat. § 3614.4; Or. Rev. Stat. § 192.547; R.I. Gen. Laws §§ 27-19-44.1, 27-20-39.1, 27-41-53.1; S.C. Code § 38-93-40; Tenn. Code § 56-7-2701.

[210] *See, e.g.*, Cal. Civ. Code § 56.17; Colo. Rev. Stat, § 10-3-1104.6; Or. Rev. Stat. §§ 192.537, -.539, -.581; Tex. Occ. Code § 56.17.

[211] National Institutes of Health, Budget (2019), *available at* https://www.nih.gov/about-nih/what-we-do/budget (last visited April 15, 2019).

[212] *Id*.

[213] National Institutes of Health, About the NIH Common Fund ("Common Fund programs address emerging scientific opportunities and pressing challenges in biomedical research that no single NIH Institute or Center (IC) can address on its own, but are of high priority for the NIH as a whole." *Available at* https://commonfund.nih.gov/ (last visited April 17, 2019).

[214] Office of the Director, Science Education, *available at* https://www.nih.gov/research-training/science-education (last visited April 17, 2019).

[215] National Library of Medicine, Office of Outreach and Special Populations in the Division of Specialized Information Services, *available at* https://sis.nlm.nih.gov/outreach/aboutresearch.html (last visited April 16, 2019).

[216] The Health Scientific Interest Group includes research resources for NIH and non-NIH scientists, *available at* https://www.gov/research-training/research-resources (last visited April 16, 2019).

[217] There are citizen science educational and collaborative projects throughout NIH. The Citizen Science Working Group is a trans-NIH collaboration. *See* https://dpcpsi.nih.gov/sites/default/files/Citizen_Science_presentation (2014) (last visited April 16, 2019).

[218] Addressing ELSI Issues in Unregulated Health Research Using Mobile Devices, Mark A. Rothstein and John T. Wilbanks, PIs, No. 1R01CA207538-01A1, National Cancer Institute, National Human Genome Research Institute, and Office of Science Policy and Office of Behavioral and Social Science Research, Office of the Director.

[219] *See, e.g.*, ReCODE Health Tools, Digital Health Decision-Making Framework and Checklist Designed for Researchers, *available at* https://recode.health/tools/ (last visited July 15, 2019) (provides information to researchers and other stakeholders interested in safe and responsible digital health research).

[220] L.O. Gostin and L.F. Wiley, *Public Health Law: Power, Duty, Restraint*, 3d ed. (Berkeley: University of California Press, 2016): 116-119.

[221] 21 C.F.R. Part 50.

[222] *Id.*

[223] *Id.* pt. 56.

[224] *Id.* pt. 54.

[225] 21 U.S.C. §§ 301-399i.

[226] *See* 21 U.S.C. § 321(h) (codifying § 201(h) of the Food, Drug, and Cosmetic Act, which defines the medical devices that Congress has authorized FDA to regulate).

[227] House Committee on Small Business, Subcommittee on Health and Technology, Mobile Medical App Entrepreneurs: Changing the Face of Health Care, June 27, 2013, *available at* https://www.himss.org/us-house-representatives-sub-committee-small-business-health-and-technology-hearing-mobile-medical (last visited November 4, 2019); Letter from Representative Marsha Blackburn, et al. to Margaret Hamburg, FDA Commissioner, and Julius Genachowski, FCC Chair, April 3, 2012, *available at* http://blackburn.house.gov/uploadedfiles/letter_from_congress_to_fda_and_fcc_-_3apr2012.pdf (last visited May 30, 2019). *See generally* C.M. Sharkey, "Direct-to-Consumer Genetic Testing: The FDA's Dual Role as Safety and Health Information Regulator," *DePaul Law Review* 68, no. 2 (2019): 343-384 (discussing FDA's changing role in regulating new technologies).

[228] Food and Drug Administration, Device Software Functions Including Mobile Medical Applications (Sept. 26, 2019), *available at* https://www.fda.gov/medical-devices/digital-health/mobile-medical-applications (last visited November 1, 2019).

[229] Pub. L. 114-255 (2016).

[230] *See* 21 U.S.C. § 360j(o)(1) (excluding five categories of software from the definition of a medical device).

[231] *Id.* at § 360j(o)(1)(B)

[232] Food and Drug Administration, General Wellness: Policy for Low Risk Devices: Guidance for Industry and Food and Drug Administration Staff (September 27, 2019), *available at* https://www.fda.gov/regulatory-information/search-fda-guidance-documents/general-wellness-policy-low-risk-devices (last visited November 1, 2019).

[233] Statement from FDA Commissioner Scott Gottlieb, M.D., and Center for Devices and Radiological Health Director Jeff Shuren, M.D., J.D., on Agency Efforts to Work with Tech Industry to Spur Innovation in Digital Health, *available at* https://www.fda.gov/news-events/press-announcements/statement-fda-commissioner-scott-gottlieb-md-and-center-devices-and-radiological-health-director (last visited Nov. 1, 2019); Food and Drug Administration, Digital Health Innovation Action Plan, *available at* https://www.fda.gov/media/106331/download (last visited November 1, 2019).

[234] Pub. L. 112-144 (2012).

[235] Food and Drug Administration, FDASIA Health IT Report: Proposed Strategy and Recommendations for a Risk-Based Framework, *available at* https://www.fda.gov/media/87886/download (last visited November 1, 2019).

[236] Federal Trade Commission, Mobile Health Apps Interactive Tool, *available at* https://www.ftc.gov/tips-advice/business-center/guidance/mobile-health-apps-interactive-tool (last visited November 1, 2019).

[237] 21 U.S.C. § 321(h).

[238] 21 C.F.R. § 801.4.

[239] *Id.*

[240] *Id.*

[241] P.B. Hutt, R.A. Merrill, and L.A. Grossman, *Food and Drug Law* 92 (4th ed. 2014).

[242] *Id.* at 96.

[243] *See* United States v. Travia, 180 F. Supp. 2d 115 (D.D.C. 2001) (providing one of the rare examples in which FDA successfully relied on circumstantial evidence to establish the intended use of a product—a drug—in a case with highly unusual facts that limit its precedential value).

[244] *See* FDA General Wellness, *supra* note 232, at 3-4 (providing examples of claims that would make a device be a medical device, as opposed to a general wellness device).

[245] *Id.* pt. 812.

[246] *Id.* § 812.2(a).

[247] L. Henley, "Clinical Investigator Training Course: How to Put Together an IDE Application," Food and Drug Administration 17 (November 14, 2013), *available at* https://www.fda.gov/media/87607/download (last visited November 1, 2019).

[248] Medical Devices; Procedures for Investigational Device Exemptions, 45 Fed. Reg. at 3735.

[249] *Id.*

[250] *Id.* at 3738.

[251] 21 U.S.C. § 396.

[252] *See* 21 C.F.R. § 812.7(a).

[253] *Id.* § 812.7(d).

[254] "Lepay: FDA to Take Closer Look at Investigator-Initiated Trial," *Guide to Good Clinical Practice Newsletter* vol. 12, no. 4, January 2008, at 1. (Thomson Publishing Group, Inc.).

[255] *See* Henley, *supra* note 247, at 12, 17.

[256] B.J. Evans, "The Limits of FDA's Authority to Regulate Clinical Research Involving High-Throughput DNA Sequencing," *Food & Drug Law Journal* 70, no. 2 (2015): 259-ii.

[257] *But cf.* N.P. Terry, "Assessing the Thin Regulation of Consumer-Facing Health Technologies," *Journal of Law, Medicine & Ethics* 48, no. 1 (Supp.) (2020): ___ (noting problems of limited coverage and weak protections).

[258] C.J. Hoofnagle, *Federal Trade Commission: Privacy Law and Policy* (Cambridge: Cambridge University Press, 2016).

[259] For a further discussion of these enforcement actions, *see* J. Wagner, "The Federal Trade Commission and Consumer Protection for Mobile Health Apps," *Journal of Law, Medicine & Ethics* 48, no. 1 (Supp.) (2020): ___-___.

[260] *Id.*

[261] Federal Trade Commission, Developing a Mobile Health App?, *available at* https://www.ftc.gov/tips-advice/business-center/guidance/mobile-health-apps-interactive-tool (last visited July 9, 2019).

[262] Consumer Product Safety Commission, Statement of Commissioner Elliot F. Kaye Regarding a Framework of Safety for the Internet of Things, January 31, 2019, *available at* https://www.cpsc.gov/s3fs-public/A_Framework_for_Safety_Across_the_Internet_of_Things_1-31-2019_0.pdf?1KJ.t4Tn04v9OtEBr2s0wyLAP.KsuuQ3 (last visited July 15, 2019).

[263] A. Glaser, "Apple Is a Tech Regulator," *Slate*, June 3, 2019, *available at* https://slate.com/technology/2019/06/apple-wwdc-sign-in-facebook-google.html?via=homepage_section_features (last visited July 15, 2019).

[264] J. Wilbanks, "Design Issues in E-Consent," *Journal of Law, Medicine & Ethics* 46, no. 1 (2018): 1-18.

[265] A. Duhaime-Ross, "Apple Makes Ethics Board Approval Mandatory for All Medical Research Apps," *The Verge*, April 29, 2015, *available at* https://www.theverge.com/2015/4/29/8513367/apple-research-kit-ethics-board-mandatory-clinical-trial (last visited July 15, 2019).

[266] N. Srnicek, *Platform Capitalism* (Cambridge, UK: Polity Press, 2017).

[267] G.G. Parker and M.W. Van Alstyne, "Two-Sided Network Effects: A Theory of Information Product Design," *Management Science* 51, no. 10 (2005): 1494-1504.

[268] *See* Wiggins and Wilbanks, *supra* note 5.

[269] D. Greene and K. Shilton., "Platform Privacies: Governance, Collaboration, and the Different Meanings of 'Privacy' in iOS and Android Development," *New Media & Society* 20, no. 4 (2018): 1640–1657, *available at* https://doi.org/10.1177/1461444817702397 (last visited July 15, 2019).

[270] J. Rajasegaran et. al, "A Multi-modal Neural Embeddings Approach for Detecting Mobile Counterfeit Apps," In L. Liu and R. White, eds., *The World Wide Web Conference (WWW '19)*. ACM, New York, NY: ACM, 2019): 3165-3171, *available at* DOI: https://doi.org/10.1145/3308558.3313427 (last visited July 15, 2019).

[271] B. Andow et al., *A Study of Grayware on Google Play. 2016 IEEE Security and Privacy Workshops (SPW)* (2016), *available at* doi:10.1109/spw.2016.40 (last visited July 15, 2019).

[272] A. Wander et al., "Energy Analysis of Public-key Cryptography for Wireless Sensor Networks," In *Third IEEE International Conference on Pervasive Computing and Communications* (IEEE): 324-328).

[273] O. Afonin, "Smartphone Encryption: Why Only 10 Per Cent of Android Smartphones Are Encrypted," *Elcom Soft Blog*, March 21, 2016, *available at* https://blog.elcomsoft.com/2016/03/smartphone-encryption-why-only-10-per-cent-of-android-smartphones-are-encrypted/ (last visited July 15, 2019).

[274] J. Porter, "Google Wants to Bring Encryption to All with Adiantum," *The Verge*, February 11, 2019, *available at* https://www.theverge.com/2019/2/11/18220019/google-adiantum-storage-encryption-android-low-power-cheap-cost (last visited July 12, 2019).

[275] B. Cyr et al., "Security Analysis of Wearable Fitness Devices (Fitbit)," *Massachusetts Institute of Technology* (2014).

[276] This is an effect in which data from a variety of sources, each of which is insufficient to reidentify someone, becomes reidentifiable when assembled or aggregated. *See* M.B. Kugler and L.J. Strahilevitz, "Actual

Expectations of Privacy, Fourth Amendment Doctrine, and the Mosaic Theory," *Supreme Court Review 2015* (2015): 205-263.

277 T. Copp, "Fitness and Fitness Tracking Devices Banned for Deployed Troops," *Military Times*, August 6, 2018), *available at* https://www.militarytimes.com/news/your-military/2018/08/06/devices-and-apps-that-rely-on-geolocation-restricted-for-deployed-troops/ (last visited July 12, 2019).

278 C. Wischhover, "A Life Insurance Company Wants to Track Your Fitness Data," *Vox*, September 20, 2018, *available at* https://www.vox.com/the-goods/2018/9/20/17883720/fitbit-john-hancock-interactive-life-insurance (last visited July 12, 2019).

279 L. Na et al., "Feasibility of Reidentifying Individuals in Large National Physical Activity Data Sets From Which Protected Health Information Has Been Removed with Use of Machine Learning," *JAMA Network Open*, published online, December 21, 2018, *available at* doi:10.1001/jamanetworkopen.2018.6040 (last visited July 12, 2019).

280 L. Foschini, "The Risk of Re-Identification of Wearable Data Is Real (And Well Known)," *Medium*, February 5, 2019), *available at* https://medium.com/@lucafoschini/https-medium-com-lucafoschini-privacy-of-wearables-data-partii-116fec6fbcf (last visited July 12, 2019).

281 E. Vayena and J. Tasioulas, "Adapting Standards: Ethical Oversight of Participant-Led Health Research," *PLoS Medicine* 10, no. 3 (2013): e1001402, *available at* https://doi.org/10.1371/journal.pmed.1001402 (last visited June 9, 2019).

282 Such a provision could be implemented by reference to a neutral standard's group's code of conduct. *See, e.g.*, CARIN Alliance Code of Conduct, *available at* https://www.carinalliance.com/our-work/trust-framework-and-code-of-conduct/ (last visited June 5, 2019).

283 These notices have been referred to as "nutrition labels." *See* C. Ciochetti, "The Future of Privacy Policies: A Privacy Nutrition Label Filled with Fair Information Practices," *John Marshall Journal of Computer and Information Law* 26, no. 1 (2009): 1-46; P.G. Kelley et al., "Standardizing Privacy Notices: An Online Study of the Nutrition Label Approach," *Proceedings of the SIGCHI Conference on Human factors in Computing Systems* (2010): 1573-1582, *available at* https://dl.acm.org/citation.cfm?id=1753561 (last visited August 19, 2019).

284 *See* L.H.S. Anaya et al., "Ethical Implications of User Perceptions of Wearable Devices," *Science and Engineering Ethics* 24, no. 1 (2018): 1-28; H. Tahir, R. Tahir, and K. McDonald-Maier, "On the Security of Consumer Wearable Devices in the Internet of Things," *PLos One* (2018), https://doi.org/10.137/journal.pone.0195487 .

285 Wooley et al., *supra* note 4; McGowan et al., *supra* note 6.

286 McGowan et al., *supra* note 6.

287 R. Bonney et al., "Next Steps for Citizen Science," *Science* 2014, no. 343 (2014):1436; A. Irwin, "Science, Public Engagement," In: J.D. Wright, ed., *International Encyclopedia of the Social and Behavioral Sciences*. (Oxford: Elsevier, 2015): 255–260.

288 B. Prainsack, "Understanding Participation: The 'Citizen Science' of Genetics," In: B. Prainsack et al., eds., *Genetics as Social Practice* (Farnham, UK: Ashgate, 2014), 147–164.

289 McGowan et al., *supra* note 6.

290 *Id.*

291 Wooley et al., *supra* note 4.

292 DIY Bio, Draft DIY Bio Code of Ethics from North American Congress (2011), *available at* https://diybio.org/codes-of-ethics-north-american-congress-2011 (last visited June 14, 2019).