It's the Wild, Wild West: Lessons Learned From IRB Members' Risk Perceptions Toward Digital Research Data

JINA HUH-YOO, Department of Information Science Drexel University, USA
EMILEE RADER, Department of Media and Information Michigan State University, USA

Digital technology that is prevalent in people's everyday lives, including smart home devices, mobile apps and social media, increasingly lack regulations for how the user data can be collected, used or disseminated. The CSCW and the larger computing community continue to evaluate and understand the potential negative impacts of research involving digital technologies. As more research involves digital data, Institutional Review Boards (IRBs) take on the difficult task of evaluating and determining risks—likelihood of potential harms—from digital research. Learning more about IRBs' role in concretizing harm and its likelihood will help us critically examine the current approach to regulating digital research, and has implications for how researchers can reflect on their own data practices. We interviewed 22 U.S.-based IRB members and found that, for the interviewees, "being digital" added a risk. Being digital meant increasing possibilities of confidentiality breach, unintended collection of sensitive information, and unauthorized data reuse. Concurrently, interviewees found it difficult to pinpoint the direct harms that come out of those risks. The ambiguous, messy, and situated contexts of digital research data did not fit neatly into current human subjects research protection protocols. We discuss potential solutions for understanding risks and harms of digital technology and implications for the responsibilities of the CSCW and the larger computing community in conducting digital research.

CCS Concepts: • **Human-centered computing** → **Human computer interaction (HCI)**; • **Social and professional topics** → *Codes of ethics*; *Government technology policy*; • **Security and privacy** → *Privacy protections.*

Additional Key Words and Phrases: Research ethics; ethics; IRB; research ethics committee; data privacy; policy

ACM Reference Format:
Jina Huh-Yoo and Emilee Rader. 2020. It's the Wild, Wild West: Lessons Learned From IRB Members' Risk Perceptions Toward Digital Research Data. *Proc. ACM Hum.-Comput. Interact.* 4, CSCW1, Article 59 (May 2020), 22 pages. https://doi.org/10.1145/3392868

1 INTRODUCTION

After the infamous Tuskegee Syphilis Study that continued for 40 years [5], it took another 25 years for the ethical principles in the Belmont Report [33] to be adopted into the Code of Federal Regulations and the Common Rule [35], a U.S. government-wide requirement for oversight of research protocols to protect human research subjects. Before these regulations were enacted, there was no regulated oversight over human subjects research in the U.S. [12]. Institutional Review Boards (IRBs) follow federal and local laws and regulations to review, approve and monitor human subjects research activities. Members of IRBs consist of people with diverse backgrounds and

Authors' addresses: Jina Huh-Yoo, Department of Information Science, Drexel University, USA, jh3767@drexel.edu; Emilee Rader, Department of Media and Information, Michigan State University, USA, emilee@msu.edu.

2573-0142/2020/5-ART59 $15.00
https://doi.org/10.1145/3392868

expertise in scientific and nonscientific areas to properly ensure the ethical conduct of human subjects research.

Evolving information technology has drastically transformed the volume and complexity by which digital research data can be collected, analyzed, and reused. Accordingly, the Common Rule has faced criticism regarding how issues related to digital research data should be addressed, including how to apply rules designed around traditional biomedical and behavioral research for new kinds of data and problems that come with them [1]. For instance, deidentification could lessen the consequences of a data breach. However, the increased reidentifiability that machine learning facilitates could nullify traditional approaches to protecting subject data.

Adding to this complexity is people's increased use of digital technologies—social media and mobile, wearable, and sensing devices that capture sensitive personal information. Accordingly, assessing risks of digital technologies is incredibly challenging. Researchers have long discussed ethical implications of digital data being produced from today's technologies [8, 13, 25]. More recently, the Connected Open Research Ethics (CORE) project team developed tools and forums to share resources about how IRBs can improve regulatory approaches for digital health research [34]. Similarly, the PERVADE [44] team is developing metrics, decision making tools, and risk assessment methods for digital data.

Researchers who create new digital technologies and study their impacts are experiencing a critical struggle to make sense of the societal impact these technologies can bring, both positively and negatively. Despite early calls for protection of data [3], suggested guidelines on fairness in machine learning algorithms [9], and increased data breach reports [26], there are no clear, coherent guidelines, laws, or regulations in the U.S. for what concrete harms digital technology can cause, and the consequences of those harms. Additionally, interconnected influences and power dynamics in business, politics, and the tech industry all contribute to the lack of clarity and transparency in regulating digital data privacy and ethics.

To seek solutions to these challenges, we interviewed IRB members in the United States. IRB members bring valuable voices to this problem, given that they can share the most direct experiences of assessing risks and regulating digital research for human subjects protection. In addition, IRBs in the U.S. are an example of a regulatory body charged with enacting federal laws designed to require transparency from public sector researchers about their data practices, in order to protect people from harm. Private sector laws with similar goals have been slow to emerge, and the challenges faced by IRBs will likely also appear in private sector contexts.

We present how IRB members made sense of what is considered as 'digital data' and how they perceived risks of data "being digital." They shared how existing regulatory protocols broke down when overseeing digital research, because of the ambiguity and complexity that "being digital" brings. We discuss how the CSCW community can understand the risks of digital technology and minimize those risks through an intertwined approach between regulatory oversight, inspired by existing regulations of personal health information, and voluntary efforts by those who are shaping and researching digital technology.

2 BACKGROUND AND RELATED WORK

2.1 Assessing Risk in Human Subjects Research

In the context of U.S., one of the main roles of the IRB is evaluating whether the "risks to subjects are reasonable in relation to anticipated benefits" (§45 CFR 46.111(a)(2)) [35]. The word "risk" here, however, implies two distinct concepts: harm as a result of the research and the likelihood that harm will occur. IRBs must not only be knowledgeable about the possible harms that could occur in a human subjects research project, but also be able to estimate the likelihood of those harms

occurring. In assessing risk, IRBs rely on the federal regulations and ethical principles stated in the Common Rule [35] and the Belmont Report [33]. However, rather than defining possible harms and ways to evaluate their likelihood, the regulations give examples of types of harm that could arise without guidance regarding how likely those harms are. Likewise, the human subjects research ethics literature [23, 39, 48] often reiterates the categories of harm in the Belmont Report [33]: "psychological harm, physical harm, legal harm, social harm and economic harm, loss of autonomy, and any forms of injustice perpetuated through the research as forms of harm."

Given these guidelines and the information provided about research studies in IRB applications, IRB members make moral judgments in weighing the risks versus benefits of a research protocol [23, 39]. Where there is empirical evidence about the incidence of harm related to some aspect of a research protocol, IRBs can use that information for estimating the likelihood of harm as part of their review. However, in situations where there is no empirical evidence, IRB members make these assessments based on their own intuition. This presents a number of problems related to the fact that intuitions and gut feelings can be biased by the IRB members' own background and experience, which may be incomplete for reviewing a given protocol [38].

A critical concept for IRBs in making determinations about whether a research study is exempt from further review is that of "minimal risk." The Common Rule defines minimal risk as "the probability and magnitude of harm or discomfort anticipated in the research are not greater in and of themselves than those ordinarily encountered in daily life or during the performance of routine physical or psychological examinations or tests" (§45 CFR 46.102(j)) [35]. In conflating probability and magnitude of harms [16], the definition of minimal risk serves as a "threshold test" [39] with several inherent biases. It labels uncommon activities as more risky just by the nature of being uncommon. It also considers common activities—something that people "ordinarily encounter in daily life"—as having a low likelihood of harm [35]. Jordan et al. [23] criticized this gap in the rule, because it leaves open the possibility that IRB members will use personal experiences as the rubric to measure what is "ordinarily encountered in daily life." This definition also leaves the potential that high-risk daily activities of potential research participants could be considered as "minimal" because people regularly engage in them [23].

2.2 New Technologies, New Potential for Harm

Previous research pointed out the Common Rule is outdated when it comes to studies that do not involve what was traditionally considered to be "observational or interventional studies conducted at a single site" [7]. In contrast to research involving digital technologies, identifying potential harms in traditional research was more straightforward and information about them could more easily be provided up front to the IRB and to participants [7]. However, digital technologies make identifying harms more complicated. Metcalf and Crawford [30] give the example of a machine learning analysis of a large dataset, which does not fall under the definition of a traditional human subjects research intervention, and as such would likely be exempt from IRB review [37]. Seemingly harmless public datasets can be used to infer sensitive information that people may not be comfortable with sharing [20]. Because of the lack of required IRB review regulations of these datasets, the scope of the harm that can be caused can be broad and unexpected [12].

Reidentification is another potential harm that is often pointed out as being more likely when collecting and analyzing digital data like online social media datasets, highly granular location data, and movement sensors [29]. Reidentification of research participants from previously anonymized data can cause participants' identities to be exposed, which increases the likelihood of harm from the research [28]. Nevertheless, a recent study of health-related papers in the CHI literature found that most researchers only took basic steps like pseudonyms and blurring faces to disguise participants' identities [2].

In addition, it was once commonly asserted that research using publicly available data does not require consent because there is no possibility of harm; however, there are many that argue that assumption does not hold any longer [30]. Ambiguity around whether informed consent is necessary, and how to get it, is another challenge for IRBs when evaluating research using digital technologies. There are situations in which consent may be hard to obtain; however, not asking for consent to participate in research is considered a possible harm due to loss of autonomy [40].

It is also possible for data to be collected about "secondary stakeholders" who are not the primary study participants, like family members of participants about whom technologies in the home record data [43], which also brings a loss of autonomy [12].

Using commercialized digital technologies in research means participant data are shared with third parties that are not subject to IRB oversight. Participants must consent to the terms and conditions required by the platforms or services being used in the research in order to participate. These terms and conditions are far from the IRB requirements for what informed consent should look like [43]. Collecting and storing digital data from third party devices also comes with the potential for data breaches on systems outside the researchers' control which could expose confidential information, and the loss or theft of a data logging device during a research study can expose a participant to harm through unauthorized access [6]. Participants may also feel discomfort due to surveillance through their participation in the research [29].

2.3 Perspectives of Researchers and IRB Members

Despite the gaps in the IRB guidance for digital research, researchers working with digital data report that their values agree with the ethical standards in the Common Rule and the Belmont Report: they think it is important to protect participants' identities, obtain informed consent, and "do no harm" [47].

Studies that interviewed IRB members found that the members perceived new kinds of risks and harms related to research using digital technologies: reidentification [46], data breaches and other improper access to digital research data [18], and emergence of new risks due to the involvement of third party platforms [34]. Crawford et al. [11] reported members of ethical review boards found it difficult to become familiar enough with terms and conditions to understand the implications for the risks of research using commercial technology products in human subjects research. Studies also identified IRBs members' concerns about the Minimal Risk criterion and misalignment between IRB members' versus researchers' understanding of the public or private nature of digital data [11, 18].

IRB members also expressed concerns about keeping up with new research practices using technologies that change rapidly [11, 34, 46]. They reported feeling like they did not understand the technologies well enough to properly assess risks [24, 34, 46]. These problems amplify inconsistencies across IRBs' assessments [34] of research protocols involving digital technologies, on top of how a large part of IRBs' review processes involve intuition about the likelihood of harm rather than empirical evidence [38]. IRB members with more experience with new technologies may both have a more "relaxed" attitude towards protocols like informed consent [19], and also have more certainty in assessing risks [18].

Building on the literature, this paper focuses on how IRB members' intuition and understanding of digital technologies informs their risk assessments, how IRB processes amplify perceived risks and harms of digital research, and how regulating digital research breaks down with current regulatory protocols and guidelines. Our research extends beyond descriptive reporting of the problems; instead, this study surfaces the uncertainties and ambiguities of digital data that hinder the concretization of risks, harms, and resolutions that arise from the complexities in digital research.

3 METHODS

We conducted a semi-structured interview study focusing on the experiences and beliefs of members of Institutional Review Boards (IRBs) of U.S. institutions regarding evaluating research protocols that involve the collection of human subjects data using digital technologies. The International Compilation of Human Research Standards report [36] lists over 1,000 laws, regulations, and guidelines that govern human subjects research in 131 countries. The U.S. is one of the few countries that enforces regulations regarding the protection of human subjects, while other countries provide guidance only. Therefore, we scoped this study to focus on the U.S. context around its federal regulations for assessing risks and benefits of conducting human subjects research.

We recruited IRB members, whom we defined as anyone responsible for reviewing or making decisions on IRB applications, including supervisory roles (IRB director, chair, or administrator), internal and external reviewers, staff, or board members of IRBs. Ten interviewees[1] were faculty or research scientists while also serving as IRB members. Ten interviewees were professionally trained in research compliance or bioethics. Two were physicians. To collect diverse perspectives from universities with various domains and levels of research activities, we obtained a university list from the Carnegie Classification of Institutions of Higher Education [22], which categorizes universities into 'very high', 'high', and 'doctoral-professional' [21] based on the level of research activities. We excluded the institutions both authors had a conflict of interest with. We randomly selected 40 universities from each category (a total of 120 universities) during the Spring of 2019, and emailed the supervisory roles of the IRB equivalent office of the institution (e.g., IRB Director, President of Office of Research) to ask them to forward our recruitment email to their IRB members. We also posted a recruitment announcement to a website for research ethics professionals. Twenty-five potential interviewees responded with interest, two did not respond to the scheduling email, and one withdrew, for a total of 22 IRB members who participated in our study. See Table 1 for more information about the interviewees.

The recruitment material included calling for those who had worked with research protocols involving digital data—"information about human behavior using some forms of digital technology, such as Fitbit, social media, or wearable sensors"—as well as any other data in a digital format each interviewee considered to be "digital data" that captures human behavior. This open definition of "digital data" allowed us to unpack how the interviewees differentiated digital data from other forms of data they were more used to regulating in the past, and what these differences meant for evaluating the risks of digital research. Six interviewees stated they reviewed "countless" or "a lot of" cases that involved the interviewees' definition of digital technology—mostly testing and developing mobile apps, physical activity sensors (e.g., Fitbit), or devices that had GPS functionalities. Eight were able to recall a few cases that involved their definition of digital technology—similar to the definition above interviewees used, but with a broader interpretation of what is digital data. Examples include online surveys and any digital information that contained sensitive personal information (e.g., audio recording of interviews). Eight had not dealt with any IRB applications that involved digital technologies. These interviewees participated in the study despite their lack of experience because they wanted to learn more about regulating digital research, be ready to review those future applications, and to help with this research, which they considered as important for future human subjects research regulation, by sharing their opinions.

We conducted phone interviews, which were audio-recorded and transcribed using an online transcription company. The interviews were semi-structured, probing interviewees' definitions of digital data, their experiences reviewing research that involved technologies collecting digital

[1] 'Interviewees' refers to the human subjects who participated in this interview study. 'Participants' refers to human subjects of research studies in general. We will use I# to refer to individuals, where # is interviewees' de-identified index.

ID	Role (Sex)	IRB cat.	Carnegie Class.	Digital Research Experience	Background
I1	Admin (F)	Biomedical*	Hospital	A lot	Research compliance
I2	Board (M)	Biomedical	Very high	A lot	Physician
I3	Admin (M)	General*	Very high	A few	Research compliance
I4	Admin (F)	General*	State institution	A lot	Research compliance
I5	Board (M)	General*	Very high	A few	Faculty/researcher
I6	Reviewer (F)	General*	Very high	A few	Faculty/researcher
I7	Admin (F)	General*	Very high	None	Research compliance
I8	Staff (F)	Both	Very high	A lot	Research compliance
I9	Admin (F)	Both	Very high	A lot	Faculty/researcher
I10	Admin (F)	Both	Very high	A few	Research compliance
I11	Admin (F)	Social Behavioral*	Doctoral-professional	None	Faculty/researcher
I12	Admin (F)	General*	Doctoral-professional	None	Faculty/researcher
I13	Admin (F)	General*	Doctoral-professional	None	Research compliance
I14	Admin (F)	General*	High	None	Faculty/researcher
I15	Board (F)	General*	Very high	A lot	Research compliance
I16	Admin (F)	General*	High	A few	Research compliance
I17	Admin (M)	General*	Doctoral-professional	None	Faculty/researcher
I18	Admin (M)	Social Behavioral*	High	A few	Research compliance
I19	Admin (F)	Both	Very high	A few	Faculty/researcher
I20	Board (M)	Biomedical*	Very high	A few	Physician
I21	Admin (F)	General*	Doctoral-professional	None	Faculty/researcher
I22	Board (M)	Both	Doctoral-professional	None	Faculty/researcher

Table 1. The table describes: the interviewees' roles as IRB members ('Admin' refers to Chairs and Directors and 'board' refers to board members); the IRB categories they serve for (social behavioral vs. biomedical vs. general vs. both, where 'general' refers to institutions not placing distinctions between biomedical vs. social behavioral and 'both' refers to serving for both social behavioral and biomedical); their institution's level of research activity; experience with regulating or reviewing digital research; their background; and gender.

data about human behavior, and their beliefs about what can be improved about regulating digital research. The interviewees were asked to describe what they considered to be "digital technology" that captures human behavior and their level of experience working with those technologies. The interviewer also presented a brief hypothetical in-lab usability study involving using an Amazon Alexa to encourage healthy eating habits for parents and young children. We chose this case based on our preliminary observations of differing opinions across different institutions' IRBs regarding involving a third party smart home platform as part of a human subjects research protocol. By using this case, we were able to probe both experienced IRB members and non-experienced members

regarding how to evaluate a research protocol involving relatively unfamiliar digital technology. With experienced IRB members, we were able to probe the existing practices by which the risks and benefits of this case might be evaluated. With less experienced IRB members, we probed the process by which they make sense of protocols involving new and unfamiliar digital technology, as they would in their current role. We then asked the interviewees to think aloud as if they were reviewing the study. This way, we captured aspects of the interviewees' practices around assessing new forms of digital research.

The first author took the lead in coding all transcripts using NVivo 11. The co-authors coded a subset of the transcripts to establish shared understanding on the coding schemes and together conducted open inductive coding process with all codes [45]. After the initial coding, we conducted an affinity diagramming analysis [4] to further merge and group the individual codes as part of the axial coding process. Based on the results of the affinity diagramming, we then conducted theoretical coding to identify the themes regarding the challenges and opportunities around regulating digital research, and largely, digital data. This study has been determined as exempt from both co-authors' universities' IRBs. Exempt in the authors' IRB system refers to not requiring the full review by their IRB Board; the application is reviewed and approved at the IRB staff level, given the minimal risk the research data brings to the human subjects.

4 FINDINGS

Our findings describe the new challenges the IRB members we interviewed faced as they encountered research protocols which used digital technologies in new ways. Our semi-structured interviews, which asked interviewees about their experiences assessing risks and benefits of research that used "digital technology collecting human behavior", allowed them to unpack their beliefs about what "digital data" are. This activity led to discovering the interviewees' broad and open-ended definitions of digital data, and what it means to regulate digital research given its risks. By "risk," the interviewees meant the likelihood of some harm occurring. The definition of "being digital" described how the interviewees saw the risks of research using digital technologies to collect data about human behavior. Being digital meant increased likelihood of data breaches, unintended collection of sensitive information, reidentification, and unauthorized data reuse. Uncertainty in assessing risks of digital data intensified with interviewees' lack of understanding of digital technology and not being able to pinpoint concrete harms. This uncertainty then further triggered the interviewees to perceive digital data to be more risky than non-digital data.

4.1 Defining Data's Digital-ness, Risks, and Harms

The interviewees believed there are certain data types or research processes working with those data that current regulations and practices did not fully address. Digital data were at increased risk by the virtue of their uncertainty and the inability to anticipate what might come out of them. The IRB's role was to identify risks, regardless of whether they could prove concrete harms. The presence of risk itself was enough to disapprove or halt a study. Accordingly, the understanding that being digital was being risky was a critical complexity to unpack.

4.1.1 Defining digital data: Being digital is deing risky. Being digital could come from involving certain technologies or having a specific data type, which would enable certain data collection and management processes. By 'data types', the interviewees were referring not only to characteristics of the data such as what kinds of technologies were used to collect it, but also the format in which the data were stored (e.g. digital audio versus an old-fashioned tape recorder). The new digital data types, new digital technologies, and new ways of collecting, processing, and managing these data

Characterization of data in research using digital technology interviewees perceived as risky	Interviewees' perceived risks of digital data	Example harms of digital research mentioned by the interviewees
Data types that are difficult to anonymize: Location data, speech, imaging, videos, audio data	Routine data breaches	*Psychological and social harm*: e.g., sensitive, stigmatized information leaked about an individual
Real-time analytics: e.g., monitoring pain levels, identifying patterns of medicine intake, real-time tracking of someone's location	Unintended collection of sensitive information	*Economic harm*: e.g., Life 360 application leading to being fired because an employee was where they should not have been
Large scale, comprehensive, and sophisticated data analysis incorporating state-of-the-art machine learning	Increased re-identifiability	*Harm from loss of autonomy*: e.g., information about an individual derived through analytics that they did not explicitly consent to revealing
Involving third-party commercial devices, e.g., wearable sensors (Fitbit, mobile apps, cloud servers)	Unauthorized reuse of collected data	*Legal harm*: e.g., Amazon Alexa capturing mandatory reporting case

Table 2. This table shows examples of how interviewees connected various characterizations of digital data to perceived risks and harms. The first column shows examples of data types, analysis, and handling of data in digital research that the interviewees perceived as risky. The second column shows interviewees' perceived risks expressed with those examples. The third column shows potential harms interviewees shared related to the corresponding risks, connecting with the types of harms from the Belmont Report. Note that interviewees had differing opinions for which data types or methods of handling data were riskier than others. The listed harms are not mutually exclusive and might co-occur for the same data type.

together made the whole research process riskier than traditional forms of research because of the uncertainties that the newness carried (See Table 2 for the summary of this section).

Data types affect risk. When the interviewees attempted to give examples about digital data, they immediately recalled data types—sensor, imaging, video, tracking, location, or audio data—which they also associated with risks. For instance, I4, after expressing that there is "significant lack of appreciation for potential risks involved," elaborated that "sensor data, such as movement and respiratory data" were the types of data she was thinking of that bring risks:

> Maybe the better starting point is to detail the type of data collection that I've seen that specifically collects sensor data from human subjects. In my experience the type of things that I've seen are use of eye tracking devices. For example, use of sensor data for children that are otherwise in [the gym] so collecting movement data, respiratory data and so forth. –I4

Similarly, I1 described how their IRB needed to do research by reading popular news about digital data collection to learn about the risks that "imaging, videos, and things like that" can bring, because to them neither the academic literature or existing policies guided how to assess the risks of those data types:

> Not necessarily the academic literature, [but] reading the pieces that were in the more popular news about these different types of technology and different issues around

> imaging, and videos, and things like that [helped]. It wasn't written down anywhere. –I1

Other digital data types that interviewees considered as high risk included location data, speech, imaging and videos, or audio data due to their high identifiability.

New technology-enabled process affects risk. To I9, it was not just the specific data types that affected risk. It was also about being digital, defined by the process by which the data are "electronically gathered, transmitted and stored." In that sense, risks coming from data being digital became a prevalent issue to "all kinds of" today's research:

> That whole area, it's the wave of not just the future, but the present now—electronic gathering of data and storage of data, and now you could even add in sensors, [has become a] much more frequent part of all kinds of research. –I9

Others viewed that the risk with new digital data types was amplified by the new digital technologies being used by researchers, which allow data to be collected indiscriminately and routinely and be analyzed with "real-time analytics" (I1). This process would lead to large-scale, comprehensive, and sophisticated data analysis that incorporates state-of-the-art machine learning. This characteristic of digital data would then facilitate collecting more information than needed, increasing the likelihood of harm. I1 compared the example of mobile health research with "traditional methods of data collection" to illustrate the ongoing nature of the data collection in digital research:

> With more traditional methods of data collection, there's a limit to what you can collect and how often you're interacting with your study participant. Whereas, with mobile health, there's the possibility of having almost constant interaction or constant data collection. –I1

The use of new digital technology brought in the risk of involving third party technology companies as part of the data collection and management process. Examples included wearable sensors like Fitbit (I2), mobile apps (I6,19), or cloud servers (I4,10). The complicating factor was that these devices' mechanisms behind how the data are collected, processed, and stored are largely ambiguous and hidden to research participants, and researchers too. I7 gave an analogy between cars versus computers and social media:

> While you may say, "Oh, everybody knows how to drive a car," but people don't understand how a car works. And maybe people don't understand now that cars have GPSes in them and can track them and all this stuff about cars. And it's the same about computers and social media. A lot of people [general public] have no clue what information Facebook is collecting about them and delivering them to [whom]. –I7

I1 and I3 explained further complications rising out of the ambiguous, intertwined processes among terms of service, privacy policies, and the consent process in using third party technologies in research:

> People (potential human subjects) have no clue what's going on with it. There are all sorts of different methods of data collection with mobile health. People (general public) are not considering what's going on in terms of Terms of Service, privacy policies, exactly what data is being collected, and what can be determined about the person because of that data. –I1

> I mean often times it is just what information is being collected, just trying to get a grasp and understanding of what it could be recording. –I3

4.1.2 What harms can being digital bring: It's about risks. The big question then was what actual harm being digital could bring, and how to assess how likely these harms might be. The larger

scale, sophisticated, and ambiguous nature of digital data amplified perceptions of the possible harms, which might not have been prevalent in traditional research. When asked about what would be concrete examples of harms, interviewees went back to the Belmont Report's definition of harm [33]: physical, economical, psychological, social, and legal harms. None of the interviewees, however, had observed concrete harm occurring from digital research. Rather, the interviewees focused on assessing the likelihood of hypothetical harms. And these risks are, according to current U.S. rules on human research protection, to be treated as if they were harms for the purpose of reviewing and approving the study.

Activities that were perceived as potentially leading to harms included: unintended collection of sensitive information, increased re-identifiability, and unauthorized use of collected data. The reasoning behind these issues being critical risks lay in the assumption that the new technologies routinely have data breaches.

Data breaches have become routine. The interviewees mentioned they expect data breaches to occur regularly with digital data (I4,9,17,20). I17 "[couldn't] go a day without looking at any news feed or a hard paper news or whatever it might be without seeing stuff about the security of data and the concerns with that." The prevalent perception was that "usually the tech company is the first to get [data breaches]" (I20). I20 continued, "These things have been hacked before. Obviously. All the big data companies have been hacked" (I20). I4 also mentioned "we probably routinely have data breaches of precisely this type of data (facial recognition of children)." The breach could further happen through hacking (I5,6), having information online (I4,7), leaks (I4,5), and theft and misplacement (I4,7,8,9,15,21). Given the expectation that breaches are inevitable, collecting sensitive information about individuals from research and potentially allowing the breached information to be reused by unauthorized entities would be exacerbating the risks. The interviewees saw that the nature of digital research further enabled this unhealthy process.

Unintended collection of sensitive information. Interviewees discussed how they believed that the nature of digital data—ongoing data collection and collecting more information than needed—facilitated unintended collection of sensitive data. Examples of sensitive data included medical conditions (I4,9), location combined with time (I9), IP addresses (I11), incriminating information about research participants (I1,5,7,8,14), mandatory reporting cases (I1,2,4,5,7,8,15,22), or any information that researchers did not know they collected or did not intend to collect (I20). For instance, I1 gave an example of a project that put sensors in the apartments of the participants to test air quality and other things. Researchers eventually had to "scale back" the data collection, because "there were some things that if [the team] tested for and there was a positive result, [the team] would have to report it to the authorities" (I1).

I4 and I5 stated that, when answering an open-ended question, a research participant could reveal more information than needed. This is of course also possible with more traditional research protocols; however, they believed that using digital technologies would exacerbate this problem by digitally recording participants' responses.

Reidentifiability. Interviewees thought that the risks of breaches of confidentiality did not necessarily come from collecting direct personal identifiers. Indirect identifiers collected through research combined with machine learning and information about individuals online could generate sophisticated information about a person:

> Even if you're not asking things like, "What's your social security number? What's your address?" The idea of combining demographic data, particularly in small-bounded populations, in today's society, are much more likely to be identifiable by somebody than pre-internet just because of the amount of information about people that's on the internet. –I7

I4 and I16 further illustrated example scenarios about how confidentiality can be breached with indirect, peripheral information about individuals:

> There's machine learning involved with Alexa, there's explicit voice recognition and use for additional secondary Amazon purposes. –I4

> They can automatically recognize the voice of people that they've talked to before. –I16

Unauthorized reuse of data. Interviewees perceived the problem of unexpected, unauthorized reuse of collected research data occurring when the following was happening together: third party companies involved in the research, the potential for data breaches, and research participants who do not fully understand the methods by which their information might be used and shared. For instance, I15 pointed out that companies could share data with other companies without research participants knowing. Seven interviewees stressed how the data collected for research are owned by the company, not the researchers. I16 stated, "people aren't always aware of what it is they're signing on for and how their data could be used beyond what the researcher intends to do." Other potential harms that digital data could bring included "losing the integrity of the whole system and trust toward research community" (I16). For example, online forums are studied without people's consent and people then would lose trust for the forum and stop using it and "the trust in the research community fizzes" (I16). It is a harm if people lose a place to feel safe (e.g., online forum) due to mistrust that is built up from the unconsented research study having taken place. I14 and I18 mentioned reputation and potential litigation to the institution as harm when things go wrong.

During the interviews, interviewees reflected more on the increased scope of potential harms, rather than actual harms they had seen or direct knowledge about the likelihood of potential harms. Mandatory reporting, for instance, was a consequence that collecting sensitive information that could bring harm. The harm of mandatory reporting can be anything from relationship problems to jail time, but the likelihood of these specific harmful outcomes occurring was not explicitly discussed by the IRB members we interviewed.

4.1.3 Conflict and ambiguity on which data has greater risk. A part of the lack of concretization of harm could be due to confusion and conflicting opinions around possibilities of harm. Opinions varied on whether certain data types bring more risks than other data. For instance, I22 considered any data involving audio files of interviews as a "voice print,"—identifiable, high risk data: "Whenever anything's audio-recorded, then it steps up to a different classification." I12, on the other hand, considered audio interview files as a "lower digital data than you probably want[ed] to [talk] about." Similarly, I8 talked about how Alexa, a smart home speaker developed by Amazon, is low risk, if the content of data collection is benign:

> We see a lot of studies looking at Alexa or just digital assistants collecting things like, "When did you ask it to turn the lights on or off." Usually interactions with Alexa are things that we're not concerned about. –I8

I4, however, saw Alexa as a technology that would enable unintended collection of private information:

> Well my worry would be if it's uncontrolled and voice activated and you don't have the necessary safeguards to only activate at the point that the data collection is meant to take place. That opens the door for all sorts of potential disclosures that are unintended or otherwise sensitive and really inappropriate for the purposes of research. –I4

As such, the two IRB members, I8 and 4, had contrasting views about the risk of Amazon Alexa. I8 admitted their institution tends to be less conservative than other institutions and considered digital assistants are not inherently risky:

> I'm trying to think of an example of a study like that when people had concerns other than just subjects might say something untoward and somehow that might increase risk. I'm having a hard time thinking of an example of something inherently concerning about a digital assistant device study. –I8

While the term "tracking" immediately alerted some interviewees as a risk (I1), I20 did not consider that tracking apps being hacked would do any direct harm:

> One thing I've thought about a lot is direct harm to patients. Let's say someone hacks the app and searches up that Patient A walked several thousand steps and Patient B walked five thousand steps. Like, that's not actionable data. It's hard to see what their direct harm could come from that. –I20

This quote illustrates I20's view that steps information would not cause any actionable harm on its own—that it is a benign type of information. I2 similarly viewed tracking and wearable devices would not cause "direct harm," in comparison to genetic information, which should require more scrutiny:

> Genetic information requires a little bit more scrutiny. I think the wearables are a relatively new thing. I think, at least the actigraphy trackers and blood sugar monitors and things like that, there's a little less concern, because the information's really not so sensitive to be used for harm[ing] patients. –I2

I20 and I2's views on what is direct harm hinge on putting more scrutiny on physical harm over others. I22 considered, however, that a digital data breach can bring a "list of possible harms that are tremendous." For instance, I22 brought up a hypothetical breach scenario related to the use of the Life 360 application—that tracking location of family members can lead to the user being fired because the user was not where they should have been during work hours.

These contradicting perspectives about how risky digital data are, and which harms are more harmful than the others, were in fact a prevalent phenomenon that some interviewees observed within their own IRB board as well as across institutions. I5 mentioned how he and other members of the IRB board have different risk assessment views:

> I didn't regard [online survey research] as risky. Other members of the committee regarded it as risky. The [survey] questions [are] not likely to raise any risks unless somebody went out of their way to say something self-incriminating on the survey. I cannot see how [ordinary surveys] should require significant time for approval. –I5

To I5, online survey data were not different than traditional data in terms of the risks it brings in the context of "being digital." But for I11 and 14, the IP address added risks to what could have been traditional survey data. While the interviewees attempted to make sense of what digital data are and what risks and harms they bring, there was not a clear answer: "But then there's the zero order question, what are the risks? And that's still I think not clear" (I9).

4.2 Regulating Digital Research: When the Protocol Breaks

The interviewees used the Common Rule to assess risks and came up with recommendations for the research process, because that was the guideline that they were trained with and was available to them. Digital research, however, brought unfamiliar territory for the interviewees. The technology was new, and no direct guidelines were available for how to assess risk and consent human subjects. Having no regulations for digital data outside research settings contributed to the heightened challenge for IRB members. Even if new standard protocols become established, challenges will persist due to the continuously evolving nature of technologies and perception toward risk.

Interviewees often could not apply standard protocols to digital research right away, especially when involving third party devices. I17 shared the initial reaction to all the questions that came to their mind when assessing the risks of the hypothetical user study of Alexa:

> Can other people access this? Does Alexa have it? Is it just you and the parent that has it? Or you and the child? You're dealing with a minor. Does the Amazon collect all this data so they can get whenever they want? Does NSA have an opportunity to get it? I don't know the answer to those questions. –I17

These questions showed the ambiguity around who among the stakeholders will access the data—subjects, bystanders, researchers, third-party companies, and other entities (e.g., National Security Agency). Interviewees gave biomedical research as an example of traditional research data that had concrete steps and guidelines for regulation: "I think that with projects developing drugs and things like that, that's something we're used to. We know how all that works" (I1); "The informed consent process we use in medical research for interventional studies, I think, is pretty robust" (I2).

However, with digital data and new technologies, these standard protocols did not fit, and the interviewees had to develop their own spontaneous approaches. I1 shared they had to come up with the language for the informed consent from scratch:

> So pretty much every type of data collection that we were doing that wasn't just the straight up bio sample collection, we had to come up with wording for it. –I1

We have no privacy anyway, so what is added risk? Interviewees believed that the general public has little protection for privacy in their everyday lives. They pointed out the lack of preventative solutions of privacy and awareness for what privacy means to subjects, researchers, and even themselves:

> [People] use it in an everyday setting so what is it such a big deal to have it used in our research? That kind of mindset [of the researchers]. –I5

> But the whole concept of private... I don't understand, and I don't think researchers understand it. And I think very little of the public really understands what they do when they go online. –I7

A common perspective was that the general public believes "No one has privacy any more" (I20), and the standard by which their privacy is protected is very low. Accordingly, the interviewees were in a moral dilemma to find justifications and standards for how to prevent harms of digital data, which had no sanctions outside of the research settings. I15 and I7 explained this view:

> The world where all of this data is being recorded anyway, and this risk exists on a daily basis outside of research ... What is it about the research that increases the risk? And there's a need to not want to hamper really great research that involves innovative technologies by having standards that don't match today's world. –I15

> We need to protect these people [subjects] from themselves... outside the research study they're doing all this stuff [sharing private information online] anyway. –I7

Research should incorporate higher ethical standards. According to the Common Rule's definition of minimal risk, if a lack of privacy is commonplace in the everyday lives of potential research participants, then nearly any study involving collection of digital data could technically be considered as minimal risk despite the potential harms from data breaches or increased reidentifiability. At the same time, the IRB members we interviewed believed that researchers have an obligation to hold themselves to higher standards than the companies providing the platforms and technologies in everyday use (I7):

> Researchers are held to much higher standards than [how companies treat data privacy], and I think they need to have a basic understanding, as do IRBs, of what all these things mean so that participants can make [an informed] decision about being in a study. –I7

This notion of participants not understanding the mechanisms behind the technologies they use becomes a problem if participants blindly trust researchers to do good work, when researchers themselves might not know enough to anticipate and prevent harms. I6 mentioned a research participant said to I6 and the researchers "I trust that you're doing the best job you can to try to protect the data." Furthermore, participants who might not be in a place to understand the complex mechanisms behind how data are collected and used—such as children or cognitively impaired, or any individuals—run into issues around autonomy (I7,8,11).

Perceived risks change over time. The challenges of placing more structure and controls into IRB protocols for estimating the likelihood of harm, however, were that the perception for what is high risk has evolved and will continue to change over time. The dynamic risk assessment process required for digital data would conflict with any static, structured protocols and regulatory rules. I16 described how IRB considers risk of public data has changed over time:

> Back in the day a long time ago people were defining public in a way that we wouldn't now. Getting people's online identities and thinking that's anonymous. –I16

I16 continued to describe how tracking students' mood was considered minimal risk years ago, but it was before they came to have newer understanding of privacy issues:

> And that was five years ago, so it was before we actually understood all the privacy issues that should have been considered but weren't. –I16

Regarding a GPS tracking study on campus years back, I5 said that their IRB did not give enough thought to potential risks:

> I don't think we really gave enough thought to whether there would be any risks if another student hacked into to monitor everything that was going on. –I5

4.3 Challenges Regulating the Gray Area of Digital Research

Interviewees perceived that the challenge of regulating digital research was addressing "gray areas"—ambiguous areas that the interviewees did not have clear answers to. I5 pointed out that, "outside of the black and white questions, the gray areas don't have any examples. I've never seen any training documents that address really gray areas" (I5).

This view points to the dominant challenge that the interviewees had faced—digital research presented questions that do not have clear-cut answers like traditional research. Other interviewees gave examples of gray area problems, such as knowing what increases digital data's risk (I7), drawing the line between what is and is not under IRB's purview—what is mandated vs. advised (I3), whether to get consent from non-primary subjects (e.g., bystanders) (I3), or designing a transparent consent process when most stakeholders do not fully understand the ramifications of data privacy (mentioned by 17 interviewees).

Going on a 'gut'. Because of the lack of formal guidance, interviewees would "go on a gut" (I5):

> I go on a gut. I don't know how else to evaluate it, aside from that gut, because the IRB training gives either sort of a prose description which can be interpreted either narrowly the way an attorney would or very broadly the way a social science friendly reviewer would. Especially with the new regulations, I need some understanding of how to address these gray area questions, otherwise, it's just all gut. –I5

I8 also used their "gut feeling" because the institution "didn't have any hard and fast rules or policies about when something requires more data security protection" and "because I'm definitely

not an expert in anything computer-related." The lack of technology expertise, inability to pinpoint risks and harms, and vacuum of regulations for digital data privacy in everyday settings together pointed to desperate need for some structure.

Shortcomings of ongoing efforts. Knowing what other institutions do and learning from them was seen as a starting place to address the problem of assessing digital research. Two interviewees were aware of an existing project, where "on their website, sample protocols of how people have tried to address [regulating gray area of digital research]." However, I16 expressed: "but it's mostly a compilation of, 'Here's how we worked it out,' rather than being like any kind of formal guidelines," showing that formal guidelines were an ultimate goal I16 would like to see in this effort. I1 was also aware of this existing project and used an online forum for IRB members in medical research. When I1 asked a question to the forums run by these two organizations, I1 felt that "the problem with those was that, what I found is that, when I would ask questions, typically, no one had the answers" (I1). I1's response showed continued lack of solutions and clarity in the field despite ongoing efforts.

Challenges in concretizing harms. One critical challenge that interviewees had to juggle was being able to present concrete and real example harms, because "researchers often think that the IRB is just concerned with hypotheticals" (I4). To develop these case examples, I1 suggested talking to IRB members from other institutions to compile a list of concerns and plans to minimize risks and increase study feasibility. I3 talked about recording how certain data types are associated with certain risks, and how guided regulations should happen:

> We've all kind of developed a collective institutional knowledge about these things and so we see something that we've seen before and we go okay we know that location data is going to be identifiable. They gotta make sure they talk about it being identifiable. They gotta talk about how they're going to secure it and ideally de-identify it as quickly as possible. Also justify why they need that or all the location data and why not only certain times a day or something like that. –I3

The IRB staff can then make informed risk assessments building on past experiences and use structures such as "confessional tales" in ethnography (I7) to share unanticipated consequences in digital research.

The interviewees felt that the change should happen from all stakeholders, including researchers and the participants in human subjects research. Researchers should broaden their minds to "so many variables that aren't already on people's minds, like terms of use, bystander effect, all these kinds of things" (I16). I19 had noticed some institutions had a website with information about Amazon Mechanical Turk, and guidelines for research protocols that use it. I21 also shared that the helpful resource "would be a combination of very clear guidelines with tons of examples, and ways to reach out to other researchers" (I21).

I10 further wanted to "[know] the right questions to ask [the researchers] depending on the data that's being collected, if it's through an app or a sensor or whatever." Even for minimal risk studies, I10 felt a need for some formal regulation processes. I10 wanted guidance so that the IRB would be able to "ask to the study team [the right questions] before [IRB] just said, 'Yeah, this is minimal risk. This meets the criteria for approval'." I4 suggested enforced ways of working with researchers can reduce ambiguity and increase efficiency in regulation:

> Having a lot of these things in writing and being mandated by the institution [and] when you can point to a policy and say per our policy on data safety, security and so forth—it's a lot easier to face the pushback because when you suggest it, you'll have a million different reasons given to you for why it can't be done. –I4

Bringing transparency. With human subjects, during the consent process, the interviewees expressed the importance of being transparent about what we do not know, knowing what to include in the consent form, and discussing about possible risks until the subjects fully understood. The key here however was to not overburden the subjects with "a fire hose of information":

> Do not give 'em a fire hose of information but yet still adequately communicate the things we know, the things we don't know. –I6

I1 strongly emphasized the importance of the assumption we should take—that people do not think about privacy issues—and be proactive in making sure subjects understand the risks and harms: "when it comes to privacy risks, you have to [teach subjects basics of privacy] regardless of if you're dealing with technologically naïve or comfortable people. Because, people just aren't thinking about the privacy issues" (I1).

Because of the lack of guidance on data privacy for digital technologies, it is the "wild, wild west" according to one interviewee:

> It's like the wild, wild, west out there. Sensor manufacturers have no guidance on what their data feed should or should not contain. So everybody just does their own thing. –I6

The "Wild West" is a colloquialism characterizing the western U.S. in its frontier period as rough and lawless [27]. I6 used the analogy to describe the lack of regulations and laws around digital data privacy. This draws attention to the critical connection that regulating human research using digital technology brings to implications on digital data privacy regulations.

5 DISCUSSION

According to the IRB members, whose role is to identify harms and the risks associated with those harms in relation to human subjects research, the complexities involved in assessing risks and harms of digital data did not come from the data type—whether it is mobile, wearable, or social media. Rather, understanding risk and harm was about "being digital"—the process-oriented, highly interpretive, situated notion inferred by ambiguous and at times sensationalistic sources of information, such as popular media. Our findings unpack what it means for data to be "digital" and allow us to elaborate the core processes surrounding research data collection, storage and use that the interviewees feared would bring risks: data breach, unintended collection of sensitive information, re-identifiability, and unauthorized reuse.

While it was hard for interviewees to pinpoint concrete harm that came out of digital research, the harms they imagined ranged from trivial to highly dangerous, and how harmful a study might be depended on interviewees' understanding of digital technology, interpretations of what makes data "digital" and viewpoints about outcomes that might be considered harmful. These viewpoints will continue to evolve over time with changing security technologies, hacking abilities, privacy sensitivity, and experiences with new technologies. The IRB's regulatory role is to weigh harm and benefit. Because the harm was difficult to pinpoint, regulating digital research posed further challenges. Added to this ambiguity was that researchers, developers, and regulators all were perceived to have different levels of risk perception and different priorities. Even among the IRB members, the perceptions of risk varied greatly.

5.1 Call for Organic Approach to Unpacking "Being Digital"

Because of the dynamic, conflicting, and overwhelmingly confusing nature of the space in which IRB members' risk assessments must occur, we argue the solution should be a synergy between an organic perspective emphasizing sharing IRB practices, and strong consequence driven federal regulations. The former refers to how interviewees shared their hard efforts to foster focus groups

with potential participants, having long one-on-one conversations with parents of participants, walking through the research goal together with the researchers before the IRB submission, providing outreach to the students, staff, and faculty about the role of IRB, and researching local laws and regulations. These approaches altogether helped to unpack intricate complexities intertwined in how risks and harms are perceived by multiple stakeholders of digital research.

One popular request by the interviewees—resource sharing across institutions, such as informed consent forms adapted for mobile health applications—can effectively address the regulatory responsibilities and liability of the institution. However, such an approach still leaves unresolved the fundamental problem of uncertainty in assessing the likelihood of harms: unintentional collection of sensitive information, threats to participant autonomy, and unexpected—not unauthorized—reuse of data. The organic, ground-up approaches are difficult to further foster through a formulaic, standardized, tool-based structures that people can easily share and adopt across institutions. Complicating factors include the differing state regulations, local needs, cultural differences of study populations, and security and computing resource differences across universities with varying resource availabilities.

Members of the CSCW community are the leaders shaping the most cutting-edge digital technology around the world. Given this incredible burden of responsibility, the community should brainstorm how to foster the organic growth of discussions and sharing of perspectives among digital technology and research stakeholders, building on expertise in computer supported collaboration, organizational studies, and knowledge systems. Example inquiries include understanding how sociotechnical systems can be designed to enable collective sense-making of unexpected consequences and risks and harms (e.g., how to brainstorm ways in which a digital technology can generate concrete harms, and what are the likelihood of risks toward those harms); and how stakeholders of differing expertise, level of technology literacy, and interests can effectively share opinions to generate tailored rules and policies for local communities as well as broader contexts (e.g., how a CSCW research project can involve community-based participatory research methods [41] to develop the project's own protocols around data management).

5.2 "It's sort of the blind man and the elephant": Negotiating Stakeholders' Priorities Over Handling Digital Data

Depending on one's role in a digital research project—as researchers, developers, human subjects, and IRB members—how these stakeholders see risks, harms, and benefits of the research can differ widely. I9 brought up the metaphor of "the blind man and the elephant," from a story illustrating researchers' "focus on the science and making the research happen, [which] is just a different focus." I9 considered the perspectives and insights toward ethics and privacy that researchers often overlook as something the IRB can help with: "I always tell researchers, 'It's not surprising that this is not at the forefront of your mind. We're here to add that piece'."

This story, however, not only applies to the researchers, but also the developers and other stakeholders involved in digital technology research and development. Each stakeholder has a different priority and focus in approaching digital data, whether it is about maintaining liability of the institution, protecting human subjects from harm, being first to market, growing a successful business, etc. The computing community has long attempted to resolve this missing viewpoint toward ethics through integrated ethics education [42]. The issue of stakeholders not being able to see the whole elephant is not new to digital research. Digital technology, together with the increased uncertainty and possibilities of new harms has added complexity to maintaining the ethical conduct of data practices. The initiating actor—the researcher, as the one designing and conducting the research—bears an ethical duty to help the stakeholders gain a holistic understanding of the giant elephant, within the guidance of the rules and regulations governing human subjects research.

The current U.S. based regulations governing human subjects research includes a focus on expected harms and benefits. Training of researchers engaged in such research in the U.S. is framed by the inexcusable harm caused by the Tuskegee Syphilis Study [5]. These regulations are, however, not optimized for the fast evolving digital technology and the research that involves them. Technology researchers' initial impression of research-induced harm, given this framing, is often that their research is unquestionably "minimal risk" when it involves technologies used by the general public on a daily basis. This is in fact how the Common Rule defines Minimal Risk. The Minimal Risk rule considers common activities—something that people "ordinarily encounter in daily life"—as having a low likelihood of harm [35]. It also leads to the impression that uncommon activities are more risky just by the nature of being uncommon. We saw evidence that this is in fact occurring, in that some interviewees reported using their "gut feeling" to help them assess risks involved in digital research, and how ambiguity and uncertainty lead to perceived increased risk by the IRB members, without concrete harms linked to those cases.

One example of a technology that might not pose direct harm to every specific individual who uses it but is potentially harmful to certain individuals or groups is facial recognition. A dataset consisting of photos of faces scraped from publicly available websites and captured in public spaces on university campuses for the purpose of conducting facial recognition technology research was recently discovered to have been used to train a facial recognition system employed by the government in China for surveillance of ethnic minority groups [31]. However, if activities similar to these to collect public data for research purposes were submitted to an IRB at all, they would likely be considered Minimal Risk. This framing of risk in reference to everyday practices does not provide structures for IRBs to use to reason about the ways in which everyday use of digital technology has potential to cause harm.

Interviewees were concerned that norms around everyday use of potentially harmful technologies should not be allowed to set the boundaries for what is considered to be "minimal risk." Beyond whether human subjects encounter the proposed research setting in their daily lives, researchers should accept the responsibility that comes with their position of authority to reflect on the impacts their study might have and anticipate potential harms and how likely those harms might be to occur. Given the shortcoming with Common Rule on assessing risks and benefits of digital research, researchers can no longer rely on whether the research has met the review standard (e.g., getting approval from the IRB). The pace at which these federal rules can adapt and the evolution of digital technology vary greatly, showing inherent gaps between regulatory rules and ethical responsibilities that digital researchers should think about. Researchers instead should work with the research ethics committees at their institutions to brainstorm what could possibly happen if their data were to be breached, what unintentional collection of sensitive information may happen, how likely reidentification is, or what unauthorized reuse might look like. Researchers should find novel ways to brainstorm these harms with broader perspectives about how things can go wrong, taking into account the detailed mechanisms by which technology transmits and stores data, and the terms of use of any commercial technologies that are incorporated into the research.

5.3 What Researchers Can Further Do: Considering Third Party Technology Use in CSCW Research

One particular challenge for technology researchers and IRBs is the use of commercial technologies that have the capability for collecting very fine-grained data about research participants' location, movements, and behaviors. There are many opportunities to generate new knowledge and conduct beneficial research using these technologies. Because they are commercially available, the researchers using them do not need the technical expertise themselves to develop them or understand how they operate. However, requiring research participants to agree to commercial

terms of service to participate in a research project opens them up to the potential for harms that are poorly understood.

In devising the solutions to this problem, the solution should fundamentally increase transparency and strengthen research participant autonomy around digital data. The researchers overseeing participants' use of commercial technologies should ensure that they themselves are familiar with the terms of service associated with the research, and take a reasonably skeptical view when documenting any gaps or ambiguities in how those terms define data collection, sharing, and use [17]. This should be done before the study is submitted for IRB review, so that IRB members may consider it and engage in a discussion with the researchers about the likelihood of potential harms due to the use of the participants' data by the commercial technology platform and its' third party partners, or those to whom the data may be sold.

Researchers should also critically re-examine the informed consent process. The quality of the consent to participate in research varies greatly based on the backgrounds of the consenting individual, and IRB review committees have a tendency to pay attention to the content of the forms rather than process of consent [15]. The informed consent process can easily become a quick addendum to a study, such as the subject skimming the informed consent form followed by their signature before the study begins. Rather than such a one-time event, researchers can dedicate the informed consent process as a separate procedure, in which the subject and the researcher collectively make sense of the implications of using the technology. Informed consent can also be a continuous process, where, in the case of studies spanning longer duration (e.g., 3 month field deployment study), the subjects can be updated about any changes regarding how the data can be collected and reused by the stakeholders of the research (e.g., terms of use) and respond to those changes as needed.

The ambiguity of harm when using commercial technologies further hinders the foundational goal of the informed consent process, by individuals consenting without having a full understanding of potential future harms. Furthermore, a power imbalance exists between commercial technology platforms and individual users—individuals do not have much choice and control over their own information [32]. This comprises a threat to the autonomy of research participants, which is one of the harms discussed in the Belmont Report [33]. Researchers should present to both IRB and participants possible harms that might result from using the digital technology. Fiske and Hauser [14], however, discussed how researchers and IRB members should not overreact to "vanishingly small probabilities of worst-case scenarios nor under-react to highly probable, greater-than-everyday risk." To do this means finding ways to show research participants the likelihood of harm from evidence-based, known, foreseeable risks.

For research that brings "digital-ness," even minimal risk studies should establish a formal procedure to monitor for any changes outside the researcher and subjects' control, such as information that may come to light through investigations of companies regarding the company's policies and data practices, as well as the use of that data by third parties. The monitored information should be documented and used to aid future evidence-based risk assessment [14]. While formal regulations were seen by our interviewees as an ideal to strive for, the dynamic, evolving nature of the field and other power influences will make macro-level changes an ongoing challenge. Researchers should take the lead in making micro-level changes, starting with their own data practices, regularly reflecting on the whole picture—the elephant. Privacy and ethical issues of digital data are no longer specialized topics that only privacy researchers should study.

5.4 Envisioning Oversight in the Wild, Wild West

Electronic medical records, which are clearly digital data, were perceived to have "robust" regulations, and IRB members felt they could manage those studies well because they knew exactly

what the potential for harm could be. The HIPAA law consists of rules for defining harms and assessing risks for those harms. There are concrete consequences if these rules were to be broken. The HIPAA law describes: (1) Who is considered covered entities, (2) What are direct identifiers, (3) What the consent should say, (4) What defines breach, and (5) What happens when breach occurs, with specifics on how fines and the level of imprisonment are calculated [10]. This law concretized data breaches as harms, and how to assess the level of harm. Regardless of whether there are physical, legal, or psychological harms that occurred out of a data breach, the data breach itself is considered harmful and the entity who enabled the breach will incur the consequences. Accordingly, all stakeholders dealing with personal health information are extremely careful in thinking about possible ways in which harm can happen. While there are concrete rules to protect health information, the U.S. government has yet to provide regulations governing other kinds of digital data collection and use.

Similar to how the Menlo Report [12] applied principles of human protection rules to security research in information and communication technologies, it is possible to brainstorm what a law could look like to regulate digital technologies learning from the guidance provided by HIPAA. Following HIPAA's structures, the rule could entail the following: (1) How to define the scope of a covered entity (e.g., size of company, how collected data are used); (2) What data should not be collected, inferred, or shared with others without consent, above and beyond traditional notions of personally identifying information; (3) What consent should entail, when harms and benefits due to technology use may evolve over time and depend on others' use of the technology and understanding those harms and benefits requires a degree of technological literacy that sometimes researchers themselves do not possess; (4) How data breach should be identified and managed, given that the likelihood of this happening might be very low and the responsibility for the breach diffuse; and (5) What consequences might be necessary after a breach occurs, and which stakeholders would be held accountable. These questions are some starting points for the researchers to voluntarily incorporate into their data monitoring protocols and ethical standards of their research team.

6 CONCLUSION

IRB members' primary goal is to assess risks and benefits of a research study to regulate how research studies can be performed accordingly. By probing IRB members' thinking processes around how they determine risks of a research study using digital technology, our study revealed the complexities involved in assessing risks and harms of digital data. The findings revealed what IRB members' perceived increased risks might be in data "being digital." However, their experiences around assessing the likelihood of harms remained largely unknown. The study further revealed the ambiguous, uncertain characteristics of regulating digital research. This finding gave insights to how researchers can reflect on their own data practices and what regulatory enforcement policies can be made to aid effective protection of individuals from harm. Our study is timely and presents concrete future steps in shaping the Wild, Wild West of digital data.

ACKNOWLEDGMENTS

We thank Samantha Hautea, Rick Wash, and others who provided feedback during the preparation of the manuscript. We also thank the reviewers and the interviewees who were incredibly supportive and enthusiastic about the topic.

REFERENCES

[1] 2017. Federal Policy for the Protection of Human Subjects, FR DOC #2017-01058. In *Federal Register*, Vol. 82, Issue 12. Office of the Federal Register, National Archives and Records Administration, 7149–7274.

[2] Jacob Abbott, Haley MacLeod, Novia Nurain, Gustave Ekobe, and Sameer Patil. 2019. Local Standards for Anonymization Practices in Health, Wellness, Accessibility, and Aging Research at CHI. In *Proceedings of the CHI Conference on Human Factors in Computing Systems*. Paper 462. https://doi.org/10.1145/3290605.3300692

[3] Paul Baran. 1967. The Future Computer Utility. *The Public Interest* 8 (1967), 75.

[4] Hugh Beyer and Karen Holtzblatt. 1997. *Contextual Design: Defining Customer-Centered Systems*. Morgan Kaufmann.

[5] Allan M. Brandt. 1978. Racism and Research: the Case of the Tuskegee Syphilis Study. *Hastings Center Report* (1978), 21–29. https://doi.org/10.2307/3561468

[6] Samantha Breslin, Martine Shareck, and Daniel Fuller. 2019. Research Ethics for Mobile Sensing Device Use by Vulnerable Populations. *Social Science & Medicine* 232 (July 2019), 50–57. https://doi.org/10.1016/j.socscimed.2019.04.035

[7] Kyle B. Brothers, Suzanne M. Rivera, R. Jean Cadigan, Richard R. Sharp, and Aaron J. Goldenberg. 2019. A Belmont Reboot: Building a Normative Foundation for Human Research in the 21st Century. *The Journal of Law, Medicine & Ethics* 47, 1 (April 2019), 165–172. https://doi.org/10.1177/1073110519840497

[8] Amy Bruckman. 2002. Studying the Amateur Artist: A Perspective on Disguising Data Collected in Human Subjects Research on the Internet. *Ethics and Information Technology* 4, 3 (2002), 217–231. https://doi.org/10.1023/A:1021316409277

[9] Michael Butterworth. 2018. The ICO and Artificial Intelligence: The Role of Fairness in the GDPR Framework. *Computer Law and Security Review* 34, 2 (2018), 257–268. https://doi.org/10.1016/j.clsr.2018.01.004

[10] Centers for Disease Control and Prevention and others. 2003. HIPAA Privacy Rule and Public Health: Guidance from CDC and the U.S. Department of Health and Human Service. *MMWR: Morbidity and Mortality Weekly Report* 52, Suppl. 1 (2003), 1–17.

[11] Sharinne Crawford, Stacey Hokke, Jan M. Nicholson, Lawrie Zion, Jayne Lucke, Patrick Keyzer, and Naomi Hackworth. 2019. "It's Not Black and White": Public Health Researchers' and Ethics Committees' Perceptions of Engaging Research Participants Online. *Internet Research* 29, 1 (Feb. 2019), 123–143. https://doi.org/10.1108/IntR-07-2017-0278

[12] David Dittrich and Erin Kenneally. 2012. The Menlo Report: Ethical Principles Guiding Information and Communication Technology Research. https://www.caida.org/publications/papers/2012/menlo_report_actual_formatted/

[13] Casey Fiesler and Nicholas Proferes. 2018. "Participant" Perceptions of Twitter Research Ethics. *Social Media + Society* 4, 1 (March 2018), 205630511876336–14. https://doi.org/10.1177/2056305118763366

[14] Susan T. Fiske and Robert M. Hauser. 2014. Protecting Human Research Participants in the Age of Big Data. *Proceedings of the National Academy of Sciences* 111, 38 (Sept. 2014), 13675–13676. https://doi.org/10.1073/pnas.1414626111

[15] Bradford H. Gray. 1978. Complexities of Informed Consent. *The Annals of the American Academy of Political and Social Science* 437, 1 (1978), 37–48. https://doi.org/10.1177/000271627843700104

[16] Frederick Grinnell, John Z. Sadler, Victoria McNamara, Kristen Senetar, and Joan Reisch. 2017. Confidence of IRB/REC Members in Their Assessments of Human Research Risk: A Study of IRB/REC Decision Making in Action. *Journal of Empirical Research on Human Research Ethics* 12, 3 (2017), 140–149. https://doi.org/10.1177/1556264617710386

[17] Hana Habib, Yixin Zou, Aditi Jannu, Neha Sridhar, Chelse Swoopes, Alessandro Acquisti, Lorrie Faith Cranor, Norman Sadeh, and Florian Schaub. 2019. An Empirical Analysis of Data Deletion and Opt-Out Choices on 150 Websites. In *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*. USENIX Association, Santa Clara, CA. https://www.usenix.org/conference/soups2019/presentation/habib

[18] Rebecca A. Hibbin, Grace Samuel, and Gjemma E. Derrick. 2018. From "a Fair Game" to "a Form of Covert Research": Research Ethics Committee Members' Differing Notions of Consent and Potential Risk to Participants Within Social Media Research. *Journal of Empirical Research on Human Research Ethics* 13, 2 (Jan. 2018), 149–159. https://doi.org/10.1177/1556264617751510

[19] Stacey Hokke, Naomi J. Hackworth, Shannon K. Bennetts, Jan M. Nicholson, Patrick Keyzer, Jayne Lucke, Lawrie Zion, and Sharinne B. Crawford. 2019. Ethical Considerations in Using Social Media to Engage Research Participants: Perspectives of Australian Researchers and Ethics Committee Members. *Journal of Empirical Research on Human Research Ethics* 19, 7 (June 2019), 155626461985462–16. https://doi.org/10.1177/1556264619854629

[20] Marcello Ienca, Agata Ferretti, Samia Hurst, Milo Puhan, Christian Lovis, and Effy Vayena. 2018. Considerations for Ethics Review of Big Data Health Research: A Scoping Review. *PloS one* 13, 10 (Oct. 2018), e0204937–15. https://doi.org/10.1371/journal.pone.0204937

[21] Indiana University Center for Postsecondary Research. 2018. The Carnegie Classification of Institutions of Higher Education: 2018 Update Facts & Figures. http://carnegieclassifications.iu.edu/downloads/CCIHE2018-FactsFigures.pdf

[22] Indiana University Center for Postsecondary Research. 2018. The Carnegie Classification of Institutions of Higher Education: Standard Listings. Retrieved September 19, 2019 from http://carnegieclassifications.iu.edu/lookup/standard.php#standard_basic2005_list

[23] Sara R. Jordan and Phillip W. Gray. 2018. Clarifying the Concept of the "Social" in Risk Assessments for Human Subjects Research. *Accountability in Research* 25, 1 (2018), 1–20. https://doi.org/10.1080/08989621.2017.1403323

[24] Robert L. Klitzman. 2013. How IRBs View and Make Decisions about Social Risks. *Journal of Empirical Research on Human Research Ethics* 8, 3 (2013), 58–65. https://doi.org/10.1525/jer.2013.8.3.58

[25] Spyros Kokolakis. 2017. Privacy Attitudes and Privacy Behaviour: A Review of Current Research on the Privacy Paradox Phenomenon. *Computers & Security* 64 (2017), 122–134. https://doi.org/10.1016/j.cose.2015.07.002
[26] Maddie Ladner. 2018. Data Breach Notification in the United States and Territories. https://privacyrights.org/resources/data-breach-notification-united-states-and-territories
[27] Zhiqiu Lin. 2007. *Policing the Wild North-West: A Sociological Study of the Provincial Police in Alberta and Saskatchewan, 1905-32*. University of Calgary Press.
[28] Holly Fernandez Lynch, Leslie E Wolf, and Mark Barnes. 2019. Implementing Regulatory Broad Consent Under the Revised Common Rule: Clarifying Key Points and the Need for Evidence. *The Journal of Law, Medicine & Ethics* 47, 2 (July 2019), 213–231. https://doi.org/10.1177/1073110519857277
[29] Nicole A. Maher, Joeky T. Senders, Alexander F.C. Hulsbergen, Nayan Lamba, Michael Parker, Jukka-Pekka Onnela, Annelien L Bredenoord, Timothy R. Smith, and Marike L.D. Broekman. 2019. Passive Data Collection and Use in Healthcare: A Systematic Review of Ethical Issues. *International Journal of Medical Informatics* 129 (2019), 242–247. https://doi.org/10.1016/j.ijmedinf.2019.06.015
[30] Jacob Metcalf and Kate Crawford. 2016. Where are Human Subjects in Big Data Research? The Emerging Ethics Divide. *Big Data & Society* 3, 1 (2016). https://doi.org/10.1177/2053951716650211
[31] Cade Metz. 2019. Facial Recognition Tech Is Growing Stronger, Thanks to Your Face. *New York Times* (July 13 2019). https://www.nytimes.com/2019/07/13/technology/databases-faces-facial-recognition-technology.html
[32] Evgeny Morozov. 2013. The Real Privacy Problem. *MIT Technology Review* 116, 6 (2013), 32–43.
[33] National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research. 1979. *The Belmont report: Ethical Principles and Guidelines for the Protection of Human Subjects of Research*. Technical Report. https://www.hhs.gov/ohrp/regulations-and-policy/belmont-report/index.html
[34] Camille Nebeker, John Harlow, Rebeca Espinoza Giacinto, Rubi Orozco-Linares, Cinnamon S Bloss, and Nadir Weibel. 2017. Ethical and Regulatory Challenges of Research Using Pervasive Sensing and Other Emerging Technologies: IRB Perspectives. *AJOB Empirical Bioethics* 8, 4 (2017), 266–276. https://doi.org/10.1080/23294515.2017.1403980
[35] US Department of Health and Human Services. 2018. Basic HHS Policy for Protection of Human Subjects (§45 CFR 46). https://www.hhs.gov/ohrp/regulations-and-policy/regulations/common-rule/index.html
[36] Office for Human Research Protections. 2019. *International Compilation of Human Research Standards*. Technical Report. U.S. Department of Health and Human Services.
[37] Nathaniel Raymond. 2019. Reboot Ethical Review in the Age of Big Data. *Nature* 568 (2019), 277.
[38] David B Resnik. 2017. The Role of Intuition in Risk/Benefit Decision-Making in Human Subjects Research. *Accountability in Research* 24, 1 (2017), 1–29. https://doi.org/10.1080/08989621.2016.1198978
[39] David B Resnik. 2018. Risks. In *The Ethics of Research with Human Subjects: Protecting People, Advancing Science, Promoting Trust*. Springer International Publishing, 165–191.
[40] Mark A Rothstein. 2015. Ethical Issues in Big Data Health Research: Currents in Contemporary Bioethics. *The Journal of Law, Medicine, Ethics* 43, 2 (Aug. 2015), 425–429. https://doi.org/10.1111/jlme.12258
[41] Yahya Salimi, Khandan Shahandeh, Hossein Malekafzali, Nina Loori, Azita Kheiltash, Ensiyeh Jamshidi, Ameneh S. Frouzan, and Reza Majdzadeh. 2012. Is Community-Based Participatory Research (CBPR) Useful? A Systematic Review on Papers in a Decade. *International journal of preventive medicine* 3, 6 (2012), 386.
[42] Jeffrey Saltz, Michael Skirpan, Casey Fiesler, Micha Gorelick, Tom Yeh, Robert Heckman, Neil Dewar, and Nathan Beard. 2019. Integrating Ethics Within Machine-learning Courses. *ACM Trans. Comput. Educ.* 19, 4, Article 32 (Aug. 2019), 26 pages. https://doi.org/10.1145/3341164
[43] Cynthia E Schairer, Caryn Kseniya Rubanovich, and Cinnamon S. Bloss. 2018. How Could Commercial Terms of Use and Privacy Policies Undermine Informed Consent in the Age of Mobile Health? *AMA Journal of Ethics* 20, 9 (Aug. 2018), 864–872. https://doi.org/10.1001/amajethics.2018.864
[44] Katie Shilton. 2017. PERVADE. https://pervade.umd.edu
[45] Anselm Strauss and Juliet Corbin. 1994. Grounded Theory Methodology: An Overview. In *Handbook of Qualitative Research*, N. K. Denzin and Y. S. Lincoln (Eds.). Sage Publications, Inc., 273–285.
[46] Jessica Vitak, Nicholas Proferes, Katie Shilton, and Zahra Ashktorab. 2017. Ethics Regulation in Social Computing Research: Examining the Role of Institutional Review Boards. *Journal of Empirical Research on Human Research Ethics* 12, 5 (July 2017), 372–382. https://doi.org/10.1177/1556264617725200
[47] Jessica Vitak, Katie Shilton, and Zahra Ashktorab. 2016. Beyond the Belmont Principles: Ethical Challenges, Practices, and Beliefs in the Online Data Research Community. In *The ACM Conference on Computer Supported Cooperative Work Social Computing*. ACM Press, 941–953. https://doi.org/10.1145/2818048.2820078
[48] Charles Weijer. 2000. The Ethical Analysis of Risk. *The Journal of Law, Medicine & Ethics* 28, 4 (2000), 344–361. https://doi.org/10.1111/j.1748-720X.2000.tb00686.x

Received January 2020; accepted March 2020